

## Purpose Team Summaries - drafted by [gnsor-ds-pdp-purpose@icann.org](mailto:gnsor-ds-pdp-purpose@icann.org)

*This file consolidates summaries drafted by individual members of the RDS PDP Purpose Team, focusing on portions of each identified document relevant to **Registration Directory Services purpose**.*

### TABLE OF CONTENTS

1. Title: WHOIS Task Force Final Report (2003) .....	3
2. Title: WHOIS Task Force Final Report (2007) .....	5
3. Title: WHOIS Policy Review Team Final Report (2012).....	14
4. Title: 2013 RAA's Data Retention Specification Discussion Document (2014).....	15
5. Title: SAC055, WHOIS: Blind Men and an Elephant (September 2012).....	16
6. Title: Privacy & Proxy Services Accreditation PDP Final Report (2015) and GNSO Council Recommendations Report to the Board regarding Adoption of PPSAI PDP .....	17
7. Title: GAC Communiqués (also reached via this link) regarding WHOIS (2007-2015) .....	20
8. Correspondence: Article 29 WP on the data protection impact of the ICANN RAA (2013-2014) ...	21
9. Correspondence: Article 29 WP on the data protection impact of the revision of the ICANN RAA concerning accuracy and data retention of WHOIS (2012) .....	21
10. Correspondence: Article 29 WP on ICANN Procedure for Handling WHOIS Conflicts with Privacy Law (2007) .....	21
11. Correspondence: Article 29 WP on ICANN's WHOIS Database Policy (2006) .....	22
12. Title: Article 29 WP 76 Opinion 2/2003 on the application of data protection principles to WHOIS directories .....	23
13. Additional Article 29 WP Documents .....	23
14. Title: Article 29 WP 203 Opinion 3/2013.....	24
15. Title: Article 29 WP 20 Opinion 3/1999.....	27
16. Title: Council of Europe Declaration of the Committee of Ministers on ICANN, human rights and the rule of law (3 June 2015).....	28
17. Title: Opinion of the European Data Protection Supervisor: Europe's role in shaping the future of Internet Governance (23 June 2014).....	29
18. Title: EDPS on ICANN's public consultation on 2013 RAA Data Retention Specification Data Elements and - Legitimate Purposes for Collection and Retention (17 April 2014) .....	31
19. Title: European Commission Website: Definition and Obligations of Data Controllers .....	32
20. Title: IWG Common Position relating to Reverse Directories (Hong Kong, 15.04.1998) .....	33
21. Title: IWG Common Position on Privacy and Data Protection aspects of the Registration of Domain Names on the Internet (Crete, 4./5.05.2000) .....	34

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

22. Title: <i>IWG Common Position on Privacy and Data Protection aspects of the Publication of Personal Data contained in publicly available documents on the Internet (Crete, 4./5.05.2000)</i> .....	34
23. Title: <i>IWG Common Position on Incorporation of telecommunications-specific principles in multilateral privacy agreements: Ten Commandments to protect Privacy in the Internet World (Berlin, 13/14.09.2000)</i> .....	34
24. Title: <i>IWG Common Position on data protection aspects in the Draft Convention on cyber-crime of the Council of Europe (Berlin, 13/14.09.2000)</i> .....	35
25. <i>Relevant National Laws that may apply to gTLDs, including U.S. Anticybersquatting Consumer Protection Act (ACPA), 15 USC §1125</i> .....	35
26. Title: <i>EWG Recommendations for a Next-Generation RDS, especially</i> .....	36
27. <i>Materials: EWG Tutorials and FAQs</i> .....	38
28. Title: <i>EWG Member Statement by Perrin</i> .....	40
29. Title: <i>EWG Member Blog by Samuels</i> .....	41
30. Title: <i>Process Framework for a PDP on Next-Generation RDS</i> .....	41
31. Title: <i>Registrar Accreditation Agreement (2013)</i> .....	42
32. Title: <i>WHOIS Uniform Domain Name Dispute Resolution Policy and Rules for Uniform Domain Name Dispute Resolution Policy</i> .....	42
33. Title: <i>WHOIS New gTLD URS Policy and Rules for URS Policy</i> .....	44
34. Title: <i>WHOIS Expired Domain Deletion Policy</i> .....	44
35. Title: <i>WHOIS Inter-Registrar Transfer Policy</i> .....	45
36. <i>ICANN WHOIS Portal Knowledge Center Q&amp;A: What is WHOIS data used for?</i> .....	46
37. Title: <i>Privacy &amp; Information Security Law Blog: Article 29 Working Party Clarifies Purpose Limitation Principles</i> .....	47
38. Title: <i>U.S. NTIA Green Paper: Improvement of Technical Management of Internet Names and Addresses (1998)</i> .....	48
39. Title: <i>U.S. NTIA White Paper: Management of Internet Names and Addresses, Statement of Policy (2012)</i> .....	49
40. Title: <i>U.S. GAO INTERNET MANAGEMENT: Prevalence of False Contact Information for Registered Domain Names (2005)</i> .....	49
41. Title: <i>Anti-Phishing Working Group Advisory on Utilization of Whois Data For Phishing Site Take Down (2008)</i> .....	50

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

### 1. Title: [WHOIS Task Force Final Report \(2003\)](#)

Summarized by: [Coupet](#)

#### I. Consensus Policies: Accuracy and Bulk Access of WHOIS Data

Purpose: Data collected must be accurate and reliable, or else registrant's site should be deleted.

Illegitimate purpose: Use of bulk access WHOIS data for marketing should not be permitted.

#### II. Recommendations to ICANN and Registrars: Accuracy of WHOIS Data and Review.

Willful provision of inaccurate or unreliable information" is a material breach of the registration agreement. ICANN should encourage registrars to take steps to remind registrants of their obligations to submit and maintain complete and accurate contact data at appropriate points, including but not limited to the time of renewal of a registration.

#### III. Discussion of the WHOIS Implementation Committee's Report

"Registrants should be required to review and validate all WHOIS data upon renewal of a registration.

"At least annually, a registrar must present to the Registrant the current WHOIS information, and remind the registrant that provision of false WHOIS information can be grounds for cancellation of their domain name registration. Registrants must review their WHOIS data, and make any corrections."

The Implementation Committee construed this as a recommendation that "registrars modify their bulk WHOIS access agreements to eliminate the use of data for marketing purposes."

The Implementation Committee concluded that "there is a need to clarify the definition of "marketing purposes".

#### IV. Comments received in Response to the Policy Report

Svensson: Further clarification needed of the proposed "functional definition" of "inaccurate or unreliable contact data", "e.g. whether a registrant must be reachable through all means of contact all the time."

Mr. Jones expresses a strong feeling that the WHOIS database "MUST be kept public and must be accurate." He quotes "research" which indicates that "people who provide false or misleading information for the WHOIS Registry should NOT be allowed to keep their domains."

"The need for express recognition that some inaccuracies in the WHOIS data protect privacy without limiting access to the domain name registrants for legitimate purposes." Ms. Kleiman notes that, while registrants will provide accurate information for registry and registrar communications (renewal notices, UDRP proceedings etc.), "not every small piece of data in the WHOIS registration needs to be accurate." She suggests that unlisted telephone numbers should be able to remain private "without fear of jeopardizing a well-known human rights website."

Distinction between purely commercial gTLDs and others: Ms. Kleiman also proposes that the Task Force's recommendations on WHOIS accuracy should be tested in a "clearly commercial gTLD" first, and

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

that "special issues that apply to individuals and political organizations in other gTLDs" should be considered later.

Vittorio Bertola: While accuracy of data in the WHOIS database may be desirable, some degree of inaccuracy is unavoidable for a variety of reasons, including: burdensome procedures for updating data; the use of "minor or major alterations of contact data" as a tool to avoid spamming and personal harassment; special risks for political speakers; "the usual complexity of the world." Mr. Bertola concludes that "automatically connecting inaccurate data [...] with a fraudulent intent or unlawful behaviour is not per se acceptable." He also notes: "the WHOIS service as currently implemented by most registries is clearly illegal in a number of countries, including the European Union."

Distinction between query-based WHOIS and bulk WHOIS: Elana Broitman (register.com). Ms. Broitman points out that public, query-based WHOIS services are abused in an equal or worse manner as bulk WHOIS. She notes that "until we address this gap, there is little use in changing bulk WHOIS requirements ... as potential bulk WHOIS licensees move to abuse of public WHOIS."

Aaron Swartz notes that the WHOIS database provides invaluable information for the public, researchers, and archivists. He suggests that complete electronic copies of the data be made available for purposes of research and archival at cost.

Mr. Auerbach disagrees with the interim report in that it starts from "an irrebutable presumption, that whois data must be published for the convenience of intellectual property owners no matter how much social damage that may cause through destruction of personal privacy."

Stanley Krute of Soda Mountain, Co.,: Whois provides a minimal level of accountability. Without an accurate whois directory, the web will become a prime location for criminal activities."

Contribution of the European Commission to the general discussion of the WHOIS database raised by the Reports produced by the ICANN WHOIS Task Force

The European Commission (mid January 2003) describes the purpose of the WHOIS database as traditionally technical and operational in nature. The submission notes that the Task Force report did not define what uses are legitimate and compatible to the original purpose. The importance of limiting the amount of personal data to be collected and processed, under the European Data Privacy Directive is emphasized. Need for "differentiated" access to provide WHOIS data but without having all data available to everybody. There is support concerning accuracy of data and to limitation of bulk access, and observes that "bulk access, for any purpose (not only for direct marketing), is in principle unacceptable."

### Contribution of the International Working Group on Data Protection in Telecommunications

The International Working Group on Data Protection in Telecommunications has provided a comment (dated January 15, 2003) in response to the Task Force's Interim Report. The Working Group reaffirms its Common Position on Privacy and Data Protection aspects of the Registration of Domain Names on

## **Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)**

the Internet originally adopted in May 2000. The Working Group is "especially critical of proposals contained in the Interim Report ... to extend the search capabilities of WHOIS databases to searches for the registrant name."

### Feedback Received by the Task Force in Response to the Final Report

Privacy concerns are not addressed, therefore Task Force Report does not represent consensus and is biased in favor of IP constituency.

Danny Younger points to a first amendment right to anonymous speech recognized by the US Supreme Court. The failure of this Task Force to even consider US or European laws on anonymity and privacy is all the more reason to reject these ill-considered recommendations."

Tucows objects against any recommendations imposing obligations upon "resellers", and against the Task Force's recommendation II.D.2, which is characterized as stating "that Registrars are wholly responsible for the accuracy of the database."

Dangers to freedom of expression and privacy posed by the disclosure of personal information, on possible abuse of that information to commit frauds such as identity theft, and on international views on privacy and data protection, such as the International Working Group on Data Protections in Telecommunications' Common Position published in March 2000.

### Minority Reports: Non-Commercial Users' Constituency

The Task Force failed to recommend appropriate privacy safeguards for domain name registrants with reasonable and legitimate expectations of privacy and the Task Force failed to assess the misuses of WHOIS data. The very existence of inaccurate data suggests that there are domain name registrants who do care to safeguard their privacy and prevent the misuse of their personally identifiable information.

## **2. Title: [WHOIS Task Force Final Report \(2007\)](#)**

Summarized by: [Coupet](#)

Define the purpose of the Registered Name Holder, technical, and administrative contacts, in the context of the purpose of WHOIS, and the purpose for which the data was collected.

Use the relevant definitions from Exhibit C of the Transfers Task force report as a starting point: (from <http://www.icann.org/gns0/transfers-tf/report-exhc-12feb03.htm>):

Typically, third parties with specific inquiries or concerns will use contact records to determine who should act upon specific issues related to a domain name record. There are typically three of these contact types associated with a domain name record, the Administrative contact, the Billing contact and the Technical contact. Contact, The administrative contact should be able to answer non-technical questions about the domain name's registration and the Domain Holder. In all cases, the Administrative Contact is viewed as the authoritative point of contact for the domain name, second only to the Domain Holder.

## **Purpose Team Summaries - drafted by gns0-rds-pdp-purpose@icann.org**

**Contact, Billing:** The billing contact is the individual, role or organization designated to receive the invoice for domain name registration and re-registration fees.

**Contact, Technical:** The technical contact is the individual, role or organization that is responsible for the technical operations of the delegated zone. This contact likely maintains the domain name server(s) for the domain. The technical contact should be able to answer technical questions about the domain name, the delegated zone and work with technically oriented people in other zones to solve technical problems that affect the domain name and/or zone.

**Domain Holder:** The individual or organization that registers a specific domain name. This individual or organization holds the right to use that specific domain name for a specified period of time, provided certain conditions are met and the registration fees are paid. This person or organization is the "legal entity" bound by the terms of the relevant service agreement with the Registry operator for the TLD in question."

### OPoC Proposal

"Under this proposal, the administrative and technical contacts would no longer be displayed within the Whois system. As a result, they would no longer have a purpose within the context of Whois."

"This proposal introduces the Operational Point of Contact, which would be collected by registrars and displayed in response to Whois queries regarding specific domain names. The purpose of the operational point of contact is to resolve, or to reliably pass on data to resolve, operational issues relating to a domain name. At a minimum, this must include the resolution of issues relating to the configuration of the records associated with the domain name within a DNS name server. The operational point of contact may also be capable of resolving additional types of issues based on an agreement with the registered name holder to do so."

"The purpose of the operational contact is to resolve, or to reliably pass on data to resolve, operational issues relating to a domain name."

### Summary of task force discussion (including proposal for access to data)

Representatives of the registrar constituency proposed that such data could be made available by contacting the registrar of record for the domain name, without any new rules or policies, but be made subject to best practices. Today, registrars handle many requests for other information not published in the Whois, and they expect to handle requests to data removed from the Whois in a similar manner.

### Statement of the Commercial and Business Users Constituency

**Recommendation:** Any proposal to modify the existing WHOIS policy related to data displayed and access to data must include a process for access to non displayed data before changes in the existing practices are introduced.

One approach that could merit study is the recognition that there are hundreds of accredited registrars, and that any approach needs to take into account the burden on legitimate users of WHOIS. It may be

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

appropriate to examine the creation of a "white list" for legitimate stakeholders who need access to deal with "legitimate" purposes, such as network attacks; phishing; pharming attacks; trademark collisions, etc.

Recommendation: The OPOC proposal should be elaborated to include a pre validation of the completeness and accuracy of contact details of the OPOC at the time of registration. The RAA should also provide for periodic checking of the OPOC details and a standardized notice to the registrant, to remind them to verify the accuracy of their OPOC details, and of consequences of providing inaccurate, or failing to correct such data, such as suspension/loss of registered name.

Therefore BC supports the concept of establishing a process whereby an individual, or appropriate non commercial service entity can apply for an opt-out for the inclusion of their contact data in a publicly accessible WHOIS if their safety and security cannot be protected otherwise, as provided by the Special Circumstances Proposal.

Recommendation: The SCP should be elaborated to include a pre validation of all contact details at the time of registration for any party determined to be eligible for SC. The third party who holds the data should be required to provide accurate data for themselves and to attest that they have verified and maintain accurate contact data for the registrant. The RAA should also provide for periodic checking of the SC registrant data and procedures to require updates, or corrections.

The BC agrees that the proposal needs to be examined for scalability to the gTLD non sponsored space. In general, the BC supports the concepts provided in the SCP to rely upon outsourcing of the special circumstances application process to independent third-party vendor(s), possibly on a regionalized basis, ensuring adequate funding and outlining a simple and clear process for the application, designation and appeal of "special circumstances" request(s).

Analysis of how the issue would affect the constituency; including any financial impact on the constituency

The BC's interests are harmed by the lack of accurate WHOIS data and will be harmed by lack of access to WHOIS data, if public access to WHOIS data is changed, and if there is no suitable substitutes to ensure that legitimate users have timely access to accurate WHOIS contact data, so that they can deal with network attacks, trademark infringements; phishing and pharming attacks, as well as undertake normal use of the WHOIS database related to checking for availability of registerable names for use in setting up new web sites.

The OPOC proposal is anticipated to have an ongoing negative financial impact to users of WHOIS data, who rely on access to WHOIS data to quickly identify and contact the party responsible for cyber squatting, phishing, pharming, network attacks, and trademark infringements.

A move to web based access coupled with improved contractual terms for bulk access will represent the least invasive change to users, but will curtail data mining in displayed data. Thus, this change, as



## **Purpose Team Summaries - drafted by gns0-rds-pdp-purpose@icann.org**

recommended by the Business Constituency, provides improvements to WHOIS but without the associated harms to the interests of the Business Constituency's members.

### Statement of the Intellectual Property Constituency (IPC)

The many legitimate uses that constituency members make of Whois data are well documented in previous submissions. For most of these uses, especially those regarding protecting the intellectual property rights of companies, non-profit institutions, trade associations, and individuals, ready access to the full range of Whois data is critical. This access enables intellectual property owners to quickly contact the party responsible for the registration or use of a domain name that involves infringement of trademark or copyright, cybersquatting, or other illegal behavior. In most cases, this quick contact leads to a prompt resolution of the problem, without the need to invoke the UDRP or more formal legal processes. In those cases which do proceed to a UDRP complaint, civil litigation, or a criminal investigation, the data currently available in Whois is often essential to effective enforcement.

Basically the same holds true when constituency members access Whois for other legitimate purposes such as combating or preventing online frauds, conducting due diligence in mergers and acquisitions, and the like: quick access to contact data on registrants and their administrative and technical agents facilitates quick resolution of problems in the great majority of cases, which is in the best economic and legal interest of all parties concerned. When a quick resolution is not possible, Whois data plays an important role in the service of legal process, further investigations, and other follow-on activities.

Under the OPOC proposal, most of the data in Whois that enables these quick contacts and that supports these follow-on activities would no longer be available to IPC members (or any other member of the public). Only the registrant's name and country/state or province would be published. Instead, the intellectual property right holder would have to work through whomever the registrant had designated as his/her/its "operational point of contact." This entity's "purpose" would be "to resolve, or to reliably pass on data to resolve, operational issues relating to a domain name." But the proposal raises far more questions than it answers about how an intellectual property right holder would achieve the quick contact with the registrant which the current system of public access facilitates.

### Statement of the Registry Constituency

RyC believes that complete anonymity, even if it were possible to achieve, is not a viable option as a mechanism for privacy protection.

Proposals for "tiered access" are examples of mechanisms for this purpose. These appear to offer significant improvements in the protection of personal privacy, as compared to the situation today. RyC recommends that the task force direct its future efforts to finding a workable form of tiered access that might be acceptable to most, if not all, interested parties. (RyC's comments on a proposal for another mechanism, the "Special Circumstances Proposal" are set forth below.)

### THE ISSUES NOT AGREED

The two issues not agreed, i.e., the purpose of WHOIS contacts, and the question whether there should



## Purpose Team Summaries - drafted by gns0-rds-pdp-purpose@icann.org

be a change in data from that now published, are unlikely ever to be the subject even of rough consensus among the interested parties.

The GNSO resolution on the subject of the purpose, adopted on April 12, 2006, reads as follows:

"The purpose of the gTLD WHOIS service is to provide information sufficient to contact a responsible party for a particular gTLD domain name who can resolve, or reliably pass on data to a party who can resolve, issues related to the configuration of the records associated with the domain name within a DNS name server." [11]

This resolution is supported by RyC with the qualification that it does not preclude access to data by law enforcement and other parties having legitimate needs for access.

RyC believes that a decent respect for registrants' interests in protection of personal privacy demands a change in the type of data published in the WHOIS service. There is, of course, a difference between the types of data collected by registrars, and the types of data published in the WHOIS service. RyC generally supports the concepts underlying the Registrar Constituency's OPoC proposal (although there are some practical concerns addressed below). Registrars have their own business needs for collection of registrant data, and should be able to make decisions primarily based on these needs and on the legal requirements of the jurisdictions where they operate.

RyC strongly believes that there is no acceptable reason for publication of an individual's personal data such as home address, phone number or email address, whether by a registry or registrar. To the extent that such data is needed for law enforcement purposes or for the resolution of conflicts such as intellectual property, the appropriate means to meet these needs should be a tiered access process.

Adoption of the positions advocated by RyC would assist the members of the RyC in fulfilling their legal obligations in their respective jurisdictions, and would be of significant benefit through lifting burdensome contractual requirements. The impact of WHOIS changes is larger for thick registries than it is for thin, and the impact on sponsored registries can be more significant than on unsponsored registries. Any major changes would likely have considerable impact on registries and especially on registrars, in time, money and resources.

### Statement of the Non Commercial Users Constituency

The Noncommercial Users Constituency (NCUC) believes that ICANN policies governing the publication of Whois data must be reformed, and quickly. The Operational Point of Contact Proposal ("OPoC Proposal") presented in this Whois Task Force Report is not perfect, but it is the only way to bring some consensus and closure to a problem that has festered for too long.

NCUC believes that the Operational Point of Contact (OPoC) Proposal is a judicious compromise that feasibly balances constituency input with the original purpose of Whois, ICANN's Mission and Core Values, and the GNSO Council's April 12 decision.

## **Purpose Team Summaries - drafted by gns0-rds-pdp-purpose@icann.org**

On the question of access to data not published, NCUC agrees with the registrars that there are existing procedures for requesting such data from the registrar of record. But we would like to see the rights of individual registrants made clearer and stronger, and we do not believe that registrars should be able to handle any form of disclosure at their own discretion. We believe that disclosure pursuant to law protects the registrars, registries and ICANN. Registrar policies should follow those that already exist in their countries for disclosure of unlisted telephone numbers, email and chatroom identities, etc.

At this time, NCUC cannot support a proposal to allow unpublished Whois data to be accessed by anyone who signs a contract agreeing to limitations on the use of the data. Although we recognize that sufficiently restrictive terms and conditions might make such a "tiered access" contract worth considering, we believe that such a policy of access must follow implementation of the OPoC proposal and be part of a new and separate PDP. Discussion of such a proposal must be linked to discussions about what data is collected by registrars; what fees should be charged to users of a tiered access regime (fees being justified both to finance the system, assign costs to cost-causers, and to discourage misuse of tiered access for unmotivated "fishing expeditions"); what limitations should be imposed on use and transfer of the data; what mechanisms would be used to enforce the contract; what kind of entities would be eligible for such contracts, what type of penalties should be imposed for abuse, and what types of access are allowed under national laws.

NCUC has always maintained that better privacy protection can pave the way for more accurate data, and therefore supports the OPoC proposal's accuracy improvement measures. Our support for improved accuracy is still contingent, however, upon a movement away from indiscriminate publication of sensitive contact data.

### Statement of the Internet Service Providers and Connectivity Providers Constituency

The ISPCP stresses the need for balance in adoption of changes, respect for earnest privacy concerns and concern over the limiting access as a means to conceal the identity of organizations or persons involved in illegal or criminal activity.

Internet Service Providers (ISPs) use Whois data for a variety of needs, but most readily to prevent and detect sources of security attacks on their respective networks and servers; to identify sources of consumer fraud, spam, phishing and denial of service attacks; and to support technical operations of their connectivity services. Moreover, since ISPs are a primary source for information on the investigation cyber-crimes, Whois data allows ISPs or law enforcement agencies to obtain some information on the subjects of the investigation that is outside the reach of ISPs but integral to obtaining the resolution of law enforcement needs.

### Full Task Force Terms of Reference

ICANN has agreements with gTLD registrars and gTLD registries that require the provision of a WHOIS service via three mechanisms: port-43, web based access, and bulk access. The agreements also require a Registered Name Holder to provide to a Registrar accurate and reliable contact details and promptly correct and update them during the term of the Registered Name registration, including: the full name,

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

postal address, e-mail address, voice telephone number, and fax number if available of the Registered Name Holder; name of authorized person for contact purposes in the case of an Registered Name Holder that is an organization, association, or corporation; the name, postal address, e-mail address, voice telephone number, and (where available) fax number of the technical contact for the Registered Name; and the name, postal address, e-mail address, voice telephone number, and (where available) fax number of the administrative contact for the Registered Name. The contact information must be adequate to facilitate timely resolution of any problems that arise in connection with the Registered Name.

A registrar is required in the Registrar Accreditation Agreement (RAA) to take reasonable precautions to protect Personal Data from loss, misuse, unauthorized access or disclosure, alteration, or destruction.

The goal of the WHOIS task force is to improve the effectiveness of the WHOIS service in maintaining the stability and security of the Internet's unique identifier systems, whilst taking into account where appropriate the need to ensure privacy protection for the Personal Data of natural persons that may be Registered Name Holders, the authorised representative for contact purposes of a Register Name Holder, or the administrative or technical contact for a domain name.

### Proposal to the Task Force by Avri Doria, Milton Mueller, Robin Gross and Wendy Seltzer

#### I) The purpose of Whois

It is widely accepted that the original gTLD Whois service was used for the purpose of coordinating technical actors as they sought to resolve operational issues related to the security and stability of the DNS and a well-functioning internet.

The importance of this original, technical purpose was reaffirmed in the GNSO council's recommended [12] definition on the purpose of Whois:

"The purpose of the gTLD Whois service is to provide information sufficient to contact a responsible party for a particular gTLD domain name who can resolve, or reliably pass on data to a party who can resolve, issues related to the configuration of the records associated with the domain name within a DNS name server."

The scope of use of published Whois data has increased considerably beyond this over time, a subject that has already been substantially considered by the GNSO Whois Task Force and Council. The scope of use of the internet has also changed over time, as have the management tools used to administer these uses.

The public debate over Whois is overlooking a very important fact. In all Whois uses related to the security and stability of the DNS, the truly useful information is not the contact information for the domain name registrant, it is the name server information for the name in question. Unfortunately, neither the contact information nor the name server information in Whois is reliable or useful, because

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

authoritative information about DNS resources doesn't live in a gTLD database, it lives inside the DNS itself.

The validity of the data in a gTLD Whois database has no impact on the operational integrity of the DNS.

Due to this disconnect between DNS and Whois, network systems managers rarely rely on gTLD Whois service when they seek to investigate or resolve serious network operations and technical coordination issues. An entirely different set of tools and resources that relies on authoritative data have evolved that support the requirements of these types of users. For example, a network administrator might use "dig"[13] or "nslookup"[14] to determine the source of a DNS problem or the network location of a mail server being abused to send spam email. All of these tools are publicly available at no charge, internet standards based, and in widespread use.

Furthermore, from a network management perspective, not only is the data in the DNS resource records more authoritative (and therefore useful), it is also more comprehensive. A typical DNS record can include information about the network location of any and all web servers, email servers and other resources associated with a specific domain name ? at all sub-levels associated with the specific DNS entry (i.e., the second, third and fourth levels of the domain hostname). The gTLD whois service contains none of this important information.

When DNS data is used in conjunction with the IP Address Whois data sourced from providers like ARIN or RIPE, a network administrator is able to form a fully authoritative view of not only the services associated with a specific domain name, but also the identity of the entity that physically hosts those resources and how to contact that entity. All of this data exists outside the gTLD Whois system.

### Technical coordination in the real world

Most technical coordination of DNS administration, abuse and network management issues occurs without ICANN's involvement. Private sector coordination is more likely through CERT, NANOG, Reg-OPS and other forums, than those operated by ICANN. These initiatives are often ad hoc and key players do often not understand the importance and value of participation. This is an area where small improvements in the overall level of cooperation between the various initiatives would lead to substantial improvement in the overall security of the internet and DNS infrastructure.

### Proposal to the Task Force by Marilyn Cade

Attempts to define the original purpose of WHOIS services encounter many disputes, according to who is speaking, whether it is a business user; an ISP/connectivity provider; a privacy activist/organization; a registry or registrar, law enforcement agency, a sys-adm dealing with network attacks; a legal advisor inside/outside a corporation.

Much of the debate on WHOIS centers around whether and what data should be publicly displayed. There has been less disagreement about the need for accurate data, and that there are legitimate uses for contact data. There are some different views on which 'Internet tools' or other resources might

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

substitute for access to accurate WHOIS data, but little exploration and there is no agreement on whether such 'tools' are indeed substitutes.

The proposal seeks to create significant changes to the display method, and therefore the access to public displayed data. Such changes can help to curtail, if not eliminate alleged and/or actual data mining and harvesting of email and telephone numbers. In addition, this proposal would, if implemented, create strict limits to how bulk access and Port 43 access to WHOIS data is granted, and the creation of a 'white list' of authorized uses, and users for bulk access.

All WHOIS access should be changed in all WHOIS services to web based access. Such web based services should include an Image Verification Check (IVC) of sufficient security strength so that the random letters generated are not easily machine readable. The requirement to implement such a system should become a part of consensus policy, but the mechanism that each registrar/registry uses for IVC should be of their selection, as long as sufficient security is ensured.

All bulk access should be moved to ICANN managed contractual terms for access, with an application/accreditation process for parties allowed to have such contracts. This consideration was first proposed by the initial DNSO WHOIS Task Force and deserves further consideration. The 'white list' should be maintained by ICANN, and will require a suitable cost based fee to bear the cost of implementation. Criteria for application/accreditation will need further examination, and should be posted for public comment as part of the development of said criteria. ICANN should develop standard terms and conditions for the agreements, and ICANN should provide enforcement when they are violated and complaints are received from the registry/registrar for such violation, including removing the accreditation for the 'white list'; such as charging additional fee penalties, etc.

In general, parties who need bulk access for legitimate purposes are trademark and other firms that provide trademark defense or portfolio management services. Consensus policy may be needed to establish the framework for collaboration to achieve a balanced solutions and terms. ICANN operational staff will play a significant role in helping to develop and implement a suitable approach.

This approach does need further exploration with law enforcement and consumer protection authorities to ensure how best to address their need for port 43 access or bulk access.

While estimates vary, approximately 75%+ of these are registered in gTLDs, and approximately 25% are registered in country codes. It is clear that while some users may find identity in a domain name as an individual, the vast majority of Internet users do not rely on domain names, but rely on ISPs, web hosters, and connectivity providers to provide them with identity online via web email addresses, individual web pages, etc. In short, what and who will support identity on the Internet is yet to be determined and continues to evolve.

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

### 3. Title: [WHOIS Policy Review Team Final Report \(2012\)](#)

Summarized by: [Rizinski](#)

I have the impression that the purpose implicitly evolves around the concept of achieving and ensuring "trust" - a term that is used a number of times throughout the document.

Many, if not all, stakeholders involved with or affected by WHOIS, may be interested in achieving and ensuring trust in the online environment (which may in turn represent a reasonable basis for achieving consensus regarding purpose), but as Chuck said, at this point we should restrain from deliberating on that topic even though it may look like a tempting starting point for discussing the fundamental question:

\*What should the over-arching purpose be of collecting, maintaining, and providing access to gTLD registration data?\*

In this context, I compiled some relevant excerpts from the final report regarding trust that we may want to consider when preparing our concise summary. The excerpts are given as follows (some parts are highlighted for improved readability and navigation throughout the excerpts):

- "The WHOIS Review Team's scope, guided by the Affirmation of Commitments was to review the extent to which ICANN's WHOIS policy and its implementation are effective, meet the legitimate needs of law enforcement and promote consumer trust." (page 6)
- "Part of the WHOIS Review Team's scope was to evaluate the extent to which ICANN's current WHOIS policy and implementation "promotes consumer trust"... This found that drivers of consumer trust include knowing the entity with whom they are dealing, and being able to find reliable contact information." (page 9)
- "...the current implementation of WHOIS services does not help to build consumer trust, and more could be done to raise awareness of the service, and to improve its user-friendliness." (page 10)\*
- "The low level of accurate WHOIS data is unacceptable, and decreases consumer trust in WHOIS..." (page 12)
- "ICANN will organize a review of WHOIS policy and its implementation to assess the extent to which WHOIS policy is effective and its implementation meets the legitimate needs of law enforcement and promotes consumer trust." (page 20)
- "The Review Team found the definition of Consumer Trust, something the ICANN Community is also exploring in the context of its policy-making processes, to be particularly challenging. Consumer Trust can be narrowly construed to mean the level of trust Internet users have in available WHOIS data; or more broadly as the level of trust consumers have in Internet information and transactions in general." (page 23)
- "Thus, lack of support of non-ASCII characters introduces an additional barrier for non-ASCII users to provide accurate and consistent domain name registration data. This has implications for their

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

tractability for law enforcement and associated organizations. Further, many people attach some pride and fondness to the correct representation of their name and other data. While this is not a purely technical or administrative requirement, it is relevant in the context of Consumer Trust." (page 46-47)

- "The Review Team was clearly told in written and oral comments that inaccurate WHOIS data can also significantly impact consumer trust and confidence in the Internet." (page 51)
- "Consumers engaged in online purchases, in our Consumer Research Study agreed: findings showed that factors which positively supported consumer trust included knowing the company with whom they were dealing with, and being able to verify their contact details online." (page 51)
- "A significant number of public responses to the WHOIS discussion paper, and input from law enforcement agencies via the review team's targeted questionnaire, argued that privacy and proxy services undermine the effectiveness of the WHOIS service, both in terms of its ability to meet the legitimate needs of law enforcement and to promote consumer trust." (page 61)
- "The GAC WHOIS Principles similarly note that WHOIS data can contribute: to user confidence in the Internet ... by helping users identify persons or entities responsible for content and services online" (page 67)
- "Part of the WHOIS Review Team's scope was to evaluate the extent to which ICANN's current WHOIS policy and implementation "promotes consumer trust". Having struggled with what "consumer" means in the context of WHOIS, and aware of the Affirmation of Commitments' observation that there are key stakeholders who do not engage in the ICANN environment, the WHOIS Review Team commissioned consumer research. This found that drivers of consumer trust include knowing the entity with whom they are dealing, and being able to find reliable contact information. The vast majority of consumers were unaware of the existence of the WHOIS service, and many struggled to understand the format of WHOIS outputs. This led us to conclude that the current implementation of WHOIS services does not help to build consumer trust, and more could be done to raise awareness of the service, and to improve its user-friendliness." (page 84)

### 4. Title: **2013 RAA's Data Retention Specification [Discussion Document](#) (2014)**

Summarized by: [Vayra](#)

This document goes through the data elements required in each section of the 2013 RAA DATA RETENTION SPECIFICATION (Sections 1.1.1 – 1.2.3) and provides potentially legitimate purposes for collection/retention of such data. In most cases, where the data is for Registrar use, legitimate purposes provided are: administration of contracts with registrant, billing, billing disputes, chargebacks, fraud prevention, to address hijacking, theft, slamming and to facilitate resolution of transfer disputes in accordance with the TDRP. Where the data is to be made public (i.e., WHOIS), legitimate purposes provided are: to address hijacking, theft, slamming and to facilitate resolution of transfer disputes in accordance with the TDRP, abuse mitigation, facilitating domain name purchases and sales.



## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

This document concludes by noting that, although law enforcement and IP concerns may not be recognized per se as legitimate purposes under the laws of some EU Member States, even law enforcement officials from various EU Member States (as well as Interpol) were strong advocates of collection and retention of data outlined in the DATA RETENTION SPECIFICATION. So, despite the differing views that may exist between privacy advocates from some government agencies and law enforcement and proprietary rights advocates from other agencies (all in the same jurisdiction), if data is retained for legitimate purposes, law enforcement's ability to access such data will likely be determined under applicable local law, e.g., pursuant to a valid subpoena or court order.

### 5. Title: [SAC055, WHOIS: Blind Men and an Elephant \(September 2012\)](#)

Summarized by: [Ferdeline](#) and [Shatan](#)

The gist of their report is that there are four current uses of the WHOIS service, two of which the SSAC says are legitimate (law enforcement access to data; security practitioner access to data), and two where it is silent on the question of legitimacy (public access to data; intellectual property owner access to data). I have bullet pointed below the main arguments they raise in relation to the purpose of collecting and maintaining this data:

- Terminology: SSAC disagrees with the term "WHOIS" - prefers three specific terms be used: domain name "registration data," "access protocol," and "directory services".
- Data Elements: The appearance of email addresses guarantees that spam will be delivered to those email addresses.
- Purpose: WHOIS was created to provide a means to make contact information available for what was then a very small (and essentially homogeneous in terms of user community) Internet compared to what exists today.
- Today there are four main uses of WHOIS:
  - Public access to details about a domain name registration. SSAC notes that "It is a widely held belief that the public Internet should have access to domain name registration data."
  - Law enforcement access to details about a domain name registration. SSAC says this is a legitimate use case.
  - Intellectual property owner access to details about a domain name registration. SSAC notes that "It is a widely held belief that intellectual property owners should have access to domain name registration data."
  - Security practitioner access to details about a domain name registration. SSAC says this is a legitimate use case.
- SSAC would like to see research into why users purchase privacy-proxy services. It has heard that some people do so to hide from law enforcement, but would like to see more research/evidence to validate this point. Privacy-proxy services should not hinder the ability to trace the identity of a domain name registrant.

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

- Access Levels: SSAC says we need to distinguish between what information is collected and what information is published in an open database. Does not comment any further.
- Universality: Whatever policy is adopted it should be applied universally across all gTLDs.
- Accuracy: Whatever data is collected must be accurate and there must be enforcement and compliance mechanisms in place to support this.

### 6. Title: [Privacy & Proxy Services Accreditation PDP Final Report \(2015\) and GNSO Council Recommendations Report to the Board regarding Adoption of PPSAI PDP](#)

Summarized by: [Aaron](#)

Below is a summary of a recently completed PDP. It is expected that the ICANN Board will approve it this year, making it a new Consensus Policy. It has to do with proxy and privacy services and the related collection and publication of contact information. It is therefore very relevant to our future discussions.

On 21 January 2016 the GNSO Council voted unanimously to approve all the recommendations contained in the Final Report from the GNSO Working Group that had been chartered to conduct a Policy Development Process (PDP) on privacy and proxy services accreditation issues. This Recommendations Report has been sent to the ICANN Board for its review, which the GNSO Council recommended be adopted by the Board. When approved by the Board the recommendations will become ICANN Consensus Policy.

The forthcoming policy covers various items including the collection of customer contact data and its publication in WHOIS, requirements for the rights and responsibilities of privacy and proxy service customers, and an accreditation program for privacy and proxy service providers. Among other things, the recommendations:

- Affirm that privacy and proxy services should be available to all registrants, whether commercial or noncommercial, individual or corporate.
- Domain contact data must be validated and verified in a manner consistent with the requirements of the 2013 RAA.
- Privacy and proxy service providers must publish their policies and procedures for when they will publish or disclose their customers' contact information (including in WHOIS), outside of the circumstances where it is required by applicable law; and
- Establish that privacy and proxy service providers should not create impediments to transfers, renewals, or restorations of domain names and should prevent publication of customer contact information during these processes.

References:

- Final Report on the Privacy & Proxy Services Accreditation Issues Policy Development Process:

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

<http://gns0.icann.org/en/issues/raa/ppsai-final-07dec15-en.pdf>

- GNSO Council Recommendations Report to the Board regarding Adoption of the Final Recommendations from the Policy Development
- Process Working Group on Privacy and Proxy Services Accreditation Issues:  
<http://gns0.icann.org/en/drafts/council-board-ppsai-recommendations-09feb16-en.pdf>

BACKGROUND: The final recommendations include the following language:

### I. DEFINITIONS

...

- "Privacy Service" means a service by which a Registered Name is registered to its beneficial user as the Registered Name Holder, but for which alternative, reliable contact information is provided by the privacy or proxy service provider for display of the Registered Name Holder's contact information in the Registration Data Service (WHOIS) or equivalent services.
- "Proxy Service" is a service through which a Registered Name Holder licenses use of a Registered Name to the privacy or proxy customer in order to provide the privacy or proxy customer use of the domain name, and the Registered Name Holder's contact information is displayed in the Registration Data Service (WHOIS) or equivalent services rather than the customer's contact information....
- "Publication" means the reveal of a person's (i.e. the licensee or beneficial owner of a registered domain name) identity/contact details in the WHOIS system.
- "Disclosure" means the reveal of a person's (i.e. the licensee or beneficial owner of a registered domain name) identity/contact details to a third party Requester without Publication in the WHOIS system.
- The term "person" as used in these definitions is understood to include natural and legal persons, as well as organizations and entities.

### II. NO DISTINCTION IN TREATMENT; WHOIS LABELING REQUIREMENTS; VALIDATION &

#### VERIFICATION OF CUSTOMER DATA:

....

II.3: The status of a registrant as a commercial organization, non-commercial organization, or individual should not be the driving factor in whether P/P services are available to the registrant. Fundamentally, P/P services should remain available to registrants irrespective of their status as commercial or non-commercial organizations or as individuals. Further, P/P registrations should not be limited to private individuals who use their domains for non-commercial purposes....

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

5. P/P customer data is to be validated and verified in a manner consistent with the requirements outlined in the WHOIS Accuracy Program Specification of the 2013 RAA (as may be updated from time to time)....

### MANDATORY PROVISIONS TO BE INCLUDED IN PROVIDER TERMS OF SERVICE & MINIMUM REQUIREMENTS TO BE COMMUNICATED TO CUSTOMERS:

6. All rights, responsibilities and obligations of registrants and P/P service customers as well as those of accredited P/P service providers need to be clearly communicated in the P/P service registration agreement, including a provider's obligations in managing those rights and responsibilities and any specific requirements applying to transfers and renewals of a domain name. In particular, all accredited P/P service providers must disclose to their customers the conditions under which the service may be terminated in the event of a transfer of the domain name, and how requests for transfers of a domain name are handled.

7. All accredited P/P service providers must include on their websites, and in all Publication and Disclosure-related policies and documents, a link to either a request form containing a set of specific, minimum, mandatory criteria, or an equivalent list of such criteria, that the provider requires in order to determine whether or not to comply with third party requests, such as for the Disclosure or Publication of customer identity or contact details.

8. All accredited P/P service providers must publish their terms of service, including pricing (e.g. on their websites). In addition to other mandatory provisions recommended by the WG, the terms should at a minimum include the following elements in relation to Disclosure and Publication:

- Clarification of when those terms refer to Publication requests (and their consequences) and when they refer to Disclosure requests (and their consequences). The WG further recommends that accredited providers expressly include a provision in their terms of service explaining the meaning and consequences of Publication.
- The specific grounds upon which a customer's details may be Disclosed or Published or service suspended or terminated, including Publication in the event of a customer's initiation of a transfer of the underlying domain name. In making this recommendation, the WG noted the changes to be introduced to the Inter Registrar Transfer Policy ("IRTP") in 2016, where following a Change of Registrant<sup>17</sup> a registrar is required to impose a 60-day inter-registrar transfer lock.
- Clarification as to whether or not a customer: (1) will be notified when a provider receives a Publication or Disclosure request from a third party; and (2) may opt to cancel its domain registration prior to and in lieu of Publication or Disclosure. However, accredited P/P service providers that offer this option should nevertheless expressly prohibit cancellation of a domain name that is the subject of a UDRP proceeding....

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

### DISCLOSURE OR PUBLICATION OF A CUSTOMER'S IDENTITY OR CONTACT DETAILS:

18. Regarding Disclosure and Publication, the WG agreed that none of its recommendations should be read as being intended to alter (or mandate the alteration of) the prevailing practice among P/P service providers to review requests manually or to facilitate direct resolution of an issue between a Requester and a P/P service customer. It also notes that disclosure of at least some contact details of the customer may in some cases be required in order to facilitate such direct resolution. In relation to Publication that is subsequently discovered to be unwarranted, the WG believes that contractual agreements between providers and their customers and relevant applicable laws will govern, and are likely to provide sufficient remedies in such instances.

19. The WG has developed an illustrative Disclosure Framework to apply to Disclosure requests made to P/P service providers by intellectual property (i.e. trademark and copyright) owners. The proposal includes requirements concerning the nature and type of information to be provided by a Requester, non-exhaustive grounds for refusal of a request, and the possibility of neutral dispute resolution/appeal in the event of a dispute. The WG recommends that a review of this Disclosure Framework be conducted at an appropriate time after the launch of the program and periodically thereafter, to determine if the implemented recommendations meet the policy objectives for which they were developed.

**7. Title:** [GAC Communiqués \(also reached via this link\) regarding WHOIS \(2007-2015\)](#) especially [GAC Principles Regarding gTLD WHOIS Services](#) (2007)  
Summarized by: [Bos](#)

The [March 2007 GAC Principles Regarding gTLD WHOIS Services](#) were published with the aim to inform and guide the work of the ICANN Board. The GAC recognised that with the evolution of the internet the WHOIS is used for public policy related activities beyond its original function (para 2.1) and stated that these should be reflected in the WHOIS definition, purpose and operation (para 3.1): providing contact points for e.g. network operators to support the security and stability of the internet (para 2.1.1), allowing users to determine the availability of domain names (para 2.1.2), assisting law enforcement authorities (which may include private parties) in investigations (para 2.1.3), assisting in combating against abusive use of ICTs including e.g. child abuse material (para 2.1.4), facilitating clearance of trademarks and countering intellectual property infringements (para 2.1.5), helping users to identify persons or entities responsible for content or services online (para 2.1.6) and assisting in combating fraud and general compliance with relevant laws (para 2.1.7).

The validity of the March 2007 GAC Principles Regarding gTLD WHOIS Services has been reconfirmed by the GAC on several occasions, including with the [April 2013 GAC 46 Beijing Communique](#) in relation to the WHOIS Expert Working Group (EWG) and in the [March 2016 GAC 55 Marrakech Communique](#) in relation to the Privacy & Proxy Services Accreditation Issues PDP Working Group.

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

The [March 2007 GAC Principles Regarding gTLD WHOIS Services](#) also recognised concerns about e.g. conflicts of WHOIS with national laws, including on privacy and data protection (para 2.2.2) and underlined the need for compliance with applicable national laws (para 3.2).

The [March 2007 GAC Principles Regarding gTLD WHOIS Services](#) also summarised that the WHOIS service should provide sufficient and accurate data about domain name registrations and registrants subject to national safeguards for individuals' privacy in a manner that 1) supports the stability, reliability, security and global interoperability of the Internet, from both a technical and public trust perspective and 2) facilitates continuous, timely and world-wide access (para 3.3).

### 8. Correspondence: Article 29 WP on the data protection impact of the ICANN RAA (2013-2014)

<https://www.icann.org/en/system/files/correspondence/namazi-to-kohnstamm-25mar14-en.pdf>

<https://www.icann.org/en/system/files/correspondence/kohnstamm-to-jeffrey-08jan14-en.pdf>

<https://www.icann.org/en/system/files/correspondence/jeffrey-to-kohnstamm-20sep13--en.pdf>

<https://www.icann.org/en/system/files/correspondence/kohnstamm-to-crocker-chehade-06jun13-en.pdf>

Summarized by: [Malancharuvil](#)

*To be provided*

### 9. Correspondence: Article 29 WP on the data protection impact of the revision of the ICANN RAA concerning accuracy and data retention of WHOIS (2012)

<https://www.icann.org/en/system/files/correspondence/kohnstamm-to-crocker-atallah-26sep12-en.pdf>

<https://www.icann.org/en/news/correspondence/chehade-to-kohnstamm-09oct12-en>

Summarized by: [Malancharuvil](#) Also [Ali](#) (p5)

*To be provided*

### 10. Correspondence: Article 29 WP on ICANN Procedure for Handling WHOIS Conflicts with Privacy Law (2007)

<http://gns0.icann.org/en/correspondence/cerf-to-schaar-24oct07.pdf>

<https://www.icann.org/en/system/files/files/cerf-to-schaar-15mar07-en.pdf>

<https://www.icann.org/en/correspondence/schaar-to-cerf-12mar07.pdf>

Summarized by: [Rizinski](#)

After reviewing the fundamental document <<https://www.icann.org/en/system/files/files/schaar-to-cerf-12mar07-en.pdf>> of this input, I extracted some relevant excerpts that are directly related to the users/purposes questions that we identified in the mind map from March 22, 2016. I highlighted some parts for improved readability and I also concisely summarized the relevant paragraphs with brief titles. The excerpts are given as follows:

- **Differentiating between legal and natural persons**

"In particular, the Article 29 WP emphasizes once more the need to differentiate between legal and natural persons registering domain names. In the first case, the publication of certain information about the company or organisation (such as their identification and their physical address) is often a

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

requirement by law in the framework of the commercial or professional activities they perform. The Article 29 WP's primary concern relates to private domain holders that use domains solely in a non-commercial context. Nevertheless, a privacy issue is at stake also for instance in a workplace with people (employees) named in the context of commercial domains." (page 2)

- **Limiting bulk access for direct marketing**

"The Working Party also reaffirms its support for earlier proposals concerning accuracy of the data (which is also one of the principles of the Data Protection Directive) published in WHOIS directories and limitation of bulk access for direct marketing issues. It recalls that bulk use of WHOIS data for direct marketing is by no means in line with the purpose for which the directories were set up and are being maintained." (page 2)

- **Distinction between publicly accessible and publicly inaccessible data**

"Introducing a distinction between publicly accessible and publicly inaccessible data, e.g. for internal purposes of registrars for billing, etc., which is typical in many national legal systems might tackle many of the problems outlined above." (page 2)

- **Definition of WHOIS purpose adopted by the GNSO Whois Task Force**

"The purpose of the gTLD Whois service is to provide information sufficient to contact a responsible party for a particular gTLD domain name who can resolve, or reliably pass on data to a party who can resolve, issues related to the configuration of the records associated with the domain name within a DNS nameserver." (page 2) Note: This is a definition adopted in the GNSO Whois Task Force Preliminary Task Force Report on Whois Services of 22 November 2006.

- **The trade-off triangle:** Technical operation of the Internet network v.s. legal responsibilities v.s. data protection and privacy rights

"The Article 29 WP acknowledges the legitimacy of the purpose of the making available of some personal data through the WHOIS services, when this publication is necessary for the technical functioning of the Internet network as set out in the purpose definition. This publicity is necessary in order to put the person running a Website in a position to face the legal and technical responsibilities which are inherent to the running of such a site. However, in its current form the database does not take account of the data protection and privacy rights of those identifiable persons who are named as the contacts for domain names and organizations."

### 11. Correspondence: Article 29 WP on ICANN's WHOIS Database Policy (2006)

<https://www.icann.org/en/system/files/files/schaar-to-cerf-22jun06-en.pdf>

<https://www.icann.org/en/correspondence/lawson-to-cerf-22jun06.pdf>

<https://www.icann.org/en/correspondence/parisse-to-icann-22jun06.pdf>

<https://www.icann.org/en/system/files/files/fingleton-to-cerf-20jun06-en.pdf>

Summarized by: **Malancharuvil**

*To be provided*



## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

### 12. Title: [Article 29 WP 76 Opinion 2/2003](#) on the application of data protection principles to WHOIS directories

Summarized by: [Vayra](#)

The most pertinent language (if any - implicit or explicit) to purpose:

- essential to determine in very clear terms what is the purpose of the Whois and which purpose(s) can be considered as legitimate and compatible to the original purpose;
- data should be relevant and not excessive for the specific purpose;
- necessary to look for less intrusive methods that would still serve the purpose of the Whois directories without having all data directly available on-line to everybody;
- data needs to be accurate; and
- data should not be used for bulk marketing.

### 13. Additional Article 29 WP Documents

[Article 29 WP 5 Recommendation 2/97](#)

[Article 29 WP 33 Opinion 5/2000](#)

[Article 29 WP 41 Opinion 4/2001](#)

[Article 29 WP 56 Working Document 5/2002](#)

[Article 29 WP 217 Opinion 4/2014](#)

Summarized by: [Vayra](#)

The most pertinent language (if any - implicit or explicit) to purpose:

[Article 29 WP 5 Recommendation 2/97](#)

- Nothing about purpose; simply takes note of the Report and Guidance by the International Working Group on Data Protection in Telecommunications ("Budapest - Berlin Memorandum on Data Protection and Privacy on the Internet"); Considers that this initiative might contribute to the improvement of the protection of fundamental rights of individuals, in particular their privacy, on a worldwide basis.

[Article 29 WP 33 Opinion 5/2000](#)

- Nothing about purpose; simply states that specific and informed consent of the subscriber must be obtained prior to the inclusion of his personal data into all kinds of public directories (traditional telephony, mobile telephony, electronic mail, electronic signatures etc.) used for reverse or multi-criteria searches. (Article 29 WP 76 Opinion 2/2003 says the same thing)

[Article 29 WP 41 Opinion 4/2001](#)

- Nothing about purpose; simply states the Council of Europe, in promoting international co-operation in matters of cyber-crime outside its own membership, needs to pay particular

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

attention to the protection of fundamental rights and freedoms, especially the right to privacy and personal data protection.

### Article 29 WP 56 Working Document 5/2002

- Nothing about purpose; this is a working document that admits to "not offer definitive solutions concerning all possible issues related to this question" of processing of personal data on the Internet by non-EU based web sites.

### Article 29 WP 217 Opinion 4/2014

- Document analyzes the criteria set down in Article 7 of Directive 95/46/EC for making data processing legitimate. Focusing on the legitimate interests of the controller, it provides guidance on how to apply Article 7(f) under the current legal framework and makes recommendations for future improvements. Article 7 requires that personal data shall only be processed if at least one of six legal grounds listed in that Article apply. In particular, personal data shall only be processed
  - (a) based on the data subject's unambiguous consent; or if -briefly put -processing is necessary for:
  - (b) performance of a contract with the data subject;
  - (c) compliance with a legal obligation imposed on the controller;
  - (d) protection of the vital interests of the data subject;
  - (e) performance of a task carried out in the public interest; or
  - (f) legitimate interests pursued by the controller, subject to an additional balancing test against the data subject's rights and interests.
- Notes that the law must "comply with data protection law, including the requirement of necessity, proportionality and purpose limitation."
- Notes that "[i]n data protection discourse, 'purpose' is the specific reason why the data are processed.

### **14. Title:** [Article 29 WP 203 Opinion 3/2013](#)

Summarized by: [Perrin](#)

#### **Importance**

This is a fundamental document wherein the WP traces the legal history of the concept of purpose limitation in data protection, from the European Convention on Human Rights (1950), through the

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

Convention 108 to the Directive 95/46 and the then current discussions on the new data protection regulation. It also analyses the way in which other fundamental concepts in data protection, such as legal basis, reasonable expectations of privacy, fairness, incompatible use, etc. interact with purpose limitation. In particular, it spells out the framework for analysis of purpose specification, namely that collection must be for specified, explicit and legitimate purposes. While prepared to enlighten the discussions on the impending regulation, it is a summary that is extremely useful to our work as it sheds light on the thinking behind the many letters and opinions from European data commissioners, which ask ICANN what is the purpose of data collection in the RAA and disclosure in the WHOIS.

### History

1950 ECHR article 8 incorporates right to privacy. Interference with right to privacy must be in accordance with law, necessary in a democratic society, and for a specified purpose (in order to judge whether interference is necessary). These principles became cornerstones of EU data protection law.

1973 Resolution (73)22 information must be appropriate and relevant re purpose for which it was stored, prohibits use for purposes other than that for which it was stored and for communication to third parties.

1974 Resolution (74)29 For public sector, purpose can be changed if “explicitly permitted by law, is granted by a competent authority, or the rules for the use of the electronic data bank are amended.”

1981 Convention 108 introduces concept of protection of personal data. Purpose limitation becomes essential principle. Article 5 sets out fundamental principles of data protection law, including lawfulness, fairness, proportionality, purpose specification and that purpose be legitimate. Also introduces incompatibility. Article 9 sets out derogations, which must be provided for by law, and necessary in a free and democratic society. Purpose limitation also in OECD Guidelines, subsequent use for different purpose only if compatible.

### Directive 95/46/EC

Public and private sector use not differentiated, so purpose specification requirements apply equally. Added that purpose must be explicit. Further processing for historical, statistical or scientific purposes not incompatible provided safeguards (eg. anonymization) are employed. States may restrict this principle in order to safeguard certain important interests if restriction is necessary. Review has found that states have implemented/interpreted this principle somewhat differently, leading to different approaches and some confusion. Test to determine incompatibility of purposes varies from “reasonable expectations” of the data subject to application of balancing tests, or other tests (eg. fairness, lawfulness, transparency).

2000/2009 European Charter of Fundamental Rights. Data protection becomes a fundamental right, distinct from privacy, and to be administered by an independent authority. Data must be processed “fairly for specified purposes” and there must be a legitimate basis for processing (by law) or with consent.

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

### Purpose Specification

Article 6(1)(b) of the Directive: data collected only for “specific, explicit and legitimate purposes”.

Purpose specification determines the data to be collected, retention periods, and all other aspects of how data is processed. Must be determined prior to or not later than collection. Each separate purpose should be specified in enough detail to be able to assess whether collection of personal data complies with law, and what safeguards are necessary.

Explicit means unambiguous, as opposed to hidden purposes. All parties (data controllers and their staff, data processors, data protection authorities and data subjects) must all be able to understand all purposes.

Legitimate is further defined in Article 7, which lays down 6 different legal grounds for data processing. However, for a purpose to be legitimate, it must also be in accordance with all provisions of applicable data protection law, as well as other applicable law such as employment law, contract law, consumer protection law, etc.

### Framework for Compatibility Assessment

Any processing following collection (eg. storage, disclosure in WHOIS) is further processing, and must meet the requirement of compatibility. The law uses the double negative (must not be incompatible). A change of purpose therefore may be permissible, providing it passes the compatibility test. Factors include:

- 1) Relationship between the purpose of collection and the purposes of further processing
- 2) Context of collection and reasonable expectations of data subjects re further use (includes concept of knowledge of data processing ecosystem)
- 3) Nature of the data and impact of further processing on data subjects (is it sensitive data, is use excessive)
- 4) Safeguards applied by data controller to ensure fair processing and prevent undue impact on data subjects (eg. anonymization, opt out, technical measures, PETS)

### Consequences of incompatibility

Legalizing an otherwise incompatible data processing activity simply by changing the terms of a contract with the data subject, or by identifying an additional legitimate interest of the controller, would go against the spirit of the purpose limitation principle and remove its substance.

### Exceptions under Article 13

Article 13 of the Directive provides that “Member states may adopt **legislative measures** to restrict the scope of the obligations and rights provided for in Article 6(1) ...when such a restriction constitutes a necessary measure to safeguard ....national security; defence; public security; the prevention, investigation, detection, and prosecution of criminal offences, or of breaches of ethics for regulated professions; an important economic or financial interest of the Member State of the European Union ...;

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

a monitoring, inspection, or regulatory function ...and the protection of the data subject or of the rights and freedoms of others. [emphasis added].

In order to understand the basic concepts of how data protection law is being interpreted with respect to registrant data, this document is useful as it explains how the concepts interrelate.

### 15. Title: [Article 29 WP 20 Opinion 3/1999](#)

Summarized by: [Ali](#)

Relevant Sections Contained Within Referenced “Opinion No 3/99 on Public sector information and the protection of personal data” by the Working Party on the protection of individuals with regard to the processing of personal data.

One of the key aspects of this opinion is the availability of public sector information. At issue is a specific category of information held by public sector bodies known as "public" information, which would be made public subject to certain rules or for a particular purpose and based, implicitly or explicitly, on the State's desire for transparency with regard to its citizens.

The objective of this Opinion is to provide input for the discussion on the protection of personal data, a dimension which must be taken into consideration when undertaking to grant greater access to public sector data, where such data relates to individuals.

THE RULES ON DATA PROTECTION APPLY TO PERSONAL DATA WHICH HAVE BEEN MADE PUBLIC  
Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data covers the principle of the right of public access to administrative documents and other factors which are relevant to the discussion The principle of purpose requires that personal data are collected for specific, explicit and legitimate purposes and are not subsequently processed in a manner which is incompatible with these purposes.

Personal data to be made public do not constitute a homogeneous category which can be dealt with uniformly from a data protection point of view. Instead, a step-by-step analysis is needed of the rights of the data subject and the right of the public to access the data respectively. While there may be public access to data, such access may be subject to certain conditions (such as proof of legitimate interest). Alternatively, the purposes for which the data may be used, for example for commercial purposes or by the media, may be restricted.

At this point it is worth mentioning that regardless of whether or not personal data are published, data subjects always has the right to access their data and, where necessary, to require that they be rectified or erased if they have not been processed in accordance with the Directive, and in particular if they are incomplete or inaccurate.

### THE NEW TECHNOLOGIES CAN HELP STRIKE A BALANCE BETWEEN THE PROTECTION OF PERSONAL DATA AND THE PUBLICATION OF SUCH DATA

In addition to promoting access to public data, in particular by providing on-line access, the new technologies and some of the accompanying administrative measures can also help to ensure compliance with the main principles of data protection, such as end purpose, the principle of

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

information, the right to object and the principle of security. However, these technologies do not provide an absolute guarantee against abuses of the principles of personal data protection described above.

Directive 95/46/EC recognises the right of data subjects to be informed about the processing of data concerning them and stipulates that at the very least they have the right to object to legitimate processing. Data subjects must therefore be informed about the commercial usage of data concerning them and must be able to object to such usage by simple and effective means.

Another possibility mentioned in the opinion was to obtain the data subject's consent for commercial usage. Data subjects must have given their consent unambiguously and in full knowledge of the facts, taking into account the fact that anyone applying for planning permission is required to submit a file which meets certain stipulations.

### CONCLUSION:

Public access to data does not mean unfettered access: all Member States base their legislation on this philosophy. When personal data are made public, either by virtue of a regulation or because the data subject himself authorises it, the data subject is not deprived of protection, ipso facto and forever. He is guaranteed such protection by law in accordance with the fundamental principles of the right to privacy.

In order to strike a balance between the right to privacy and the protection of personal data on the one hand, and the right of the general public to access public sector data on the other, conclusions must take account of the following factors and issues:

- a case-by-case assessment of whether personal data can be published/should be accessible or not, and if so, under what conditions and on which media (computerised or not, Internet dissemination or not, etc.);
- the principles of purpose and legitimacy;
- the obligation to inform the data subject;
- the data subject's right to object;
- the use of the new technologies to help protect the right to privacy.

These factors should be taken into account not just in situations where publication or access is already regulated, but also in situations where regulation does not appear necessary, with a view to satisfying the general public's demand for access to public sector information, including personal data.

### 16. Title: [Council of Europe Declaration of the Committee of Ministers on ICANN, human rights and the rule of law \(3 June 2015\)](#)

Summarized by: [Vayra](#)

- Nothing about purpose; simply states the contractual policies and services made accessible to the public by ICANN involve the processing and retention of personal data that can necessitate compliance with national law and may raise issues under Article 8 of the European Convention on Human Rights with regard to the right to private and family life.

**17. Title: [Opinion of the European Data Protection Supervisor: Europe's role in shaping the future of Internet Governance \(23 June 2014\)](#)**

Summarized by: [Allegretti](#)

On February 12, 2014 the European Commission published a Communication on Internet Policy and Governance ("the Communication") in the wake of the NSA surveillance revelation. The European Data Protection Supervisor subsequently issued an Opinion on the Communication, further discussing a number of issues addressed in the Communication.

8. With this opinion, we wish to contribute to the debate, as any reform of Internet Governance will likely have a significant impact on citizens and on their fundamental rights, not least the rights to privacy and data protection. While this Opinion addresses an issue of global nature and while it takes account of the developments at global level, it focuses on the actions that the European Union and its institutions can perform to influence the debate and the Internet Governance structures and processes themselves.

The Opinion urged that collection of data, including gTLD registration data, should be viewed in the context of privacy and data protection:

**II. PRIVACY AND DATA PROTECTION ARE STRONGLY RELATED TO GOOD INTERNET GOVERNANCE**

13. We note some positive developments at international level in recognising privacy and data protection as essential values for the internet. At the Net Mundial, a general consensus was reached on the need to protect privacy on the Internet, by pointing out that "The right to privacy must be protected. This includes not being subject to arbitrary or unlawful surveillance, collection, treatment and use of personal data. The right to the protection of the law against such interference should be ensured".

14. We therefore urge that privacy and data protection should be core elements of any Internet Governance model, and recommend that the European Union put its full weight behind initiatives ensuring that such integration process is undertaken at a global level.

**II.2 Data protection as a cornerstone for shaping Internet Governance**

16. When discussing Internet Governance, it should be kept in mind that the governance of the Internet's infrastructure and global resources such as names and addresses is not the only source for privacy risks, but that the services provided on the Internet often create even greater risks for the privacy of their users and of third parties. In order to develop a comprehensive policy for the protection of privacy on the Internet, the Union must not only look at the global processes, but also at other relevant rules and mechanisms. An example of a data protection issue which has to be addressed by the Internet governance bodies is the current WHOIS system with the authentication and data retention requirements.<sup>14</sup> On the other hand, examples of activities performed on the Internet with significant data protection implications include eCommerce, eGovernment, eHealth, eMoney, ePayments. We would like to emphasise that, in each of the above cases, privacy and data protection principles must be at the core



## Purpose Team Summaries - drafted by gns0-rds-pdp-purpose@icann.org

The Opinion notes that there is still no consensus on the collection of registration data as it relates to privacy but urges that work continue to find a replacement for the current WHOIS:

26. We welcome that ICANN has undertaken the establishment of an expert working group on directory services for generic top level domains<sup>20</sup> with a view to replacing the current WHOIS system with a solution taking account, inter alia, of privacy concerns. We also welcome the Commission's participation in this group. We take note that the EWG has so far failed to reach a full consensus in particular on privacy related issues. We urge the ICANN bodies and stakeholders to take proper account of the report and the related arguments<sup>21</sup> in the forthcoming stages of its governance process which may lead eventually to a replacement

Any requirements for the collection and use of personal data must be based on trust:

### III.2. Internet policies must reconcile security requirements and fundamental rights

37. The Communication argues that confidence in the Internet and its governance is a prerequisite for the realisation of the Internet's potential as an engine for economic growth and innovation. The safety, security, stability and resilience of the Internet are crucial to preserve and foster the economic and societal benefits of the digital ecosystem.<sup>25</sup>

38. We agree that -especially after the recent revelations about mass surveillance- there is a need to restore users' confidence in the Internet and in the use of personal data on the Internet. As indicated in our previous opinion on the Cyber Security Strategy,<sup>26</sup> we believe that, due to the ever growing use of Information and Communication Technologies, measures aimed at ensuring a high level of security on the Internet should help improve the security of all the information processed therein, including personal data. In particular, we consider that security of data processing has always been a crucial element of data protection as security requirements are included in a number of data protection provisions.<sup>27</sup> Therefore, improving the security standards of the Internet will increase the protection of users' personal data and prevent undue interference to occur. We consider that improved standardisation of network and information security requirements at international level will also help address more efficiently the needs for trust and security.

The Opinion outlines a number of suggestions which could apply to the question of who should have access to gTLD registration data and why:

39. In this respect, we welcome the clarification that security is not opposed to privacy and data protection. We recall the explicit recognition of privacy and data protection in the Cyber Security Strategy and the fact that they are considered as core values which should guide cyber security policy in the EU and internationally.

44. The Commission should promote structures and mechanisms supporting the application of both data protection-by-design and by-default as guiding principles in the shaping of a new governance model. It should therefore ensure that data protection mechanisms and safeguards are included, from the outset, in the design of normative and technical governance tools.

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

45. The Commission should also use its policy and financial instruments to support the development of technical solutions for the internet that demonstrate how privacy can be respected in internet protocols, services and applications.

The Opinion concluded with the expectation that the Commission should promote EU standards on data protection:

We expect the Commission to show leadership and act as a catalyst in the discussions on the new Internet Governance model. In particular, we encourage the Commission to promote EU standards on data protection as well as to encourage the accession by third countries to relevant international data protection standards. Furthermore, we support the adoption of an international instrument requiring the respect of data protection standards by intelligence and law enforcement bodies.

### 18. Title: [EDPS on ICANN's public consultation on 2013 RAA Data Retention Specification Data Elements and - Legitimate Purposes for Collection and Retention \(17 April 2014\)](#)

Summarized by: [Allegretti](#)

According to the European Data Protection Supervisor, the 2013 RAA and the Draft Specification do not comply with European data protection law and he states that personal data should only be collected to perform the contract between Registrar and Registrant, and it should be retained no longer than is necessary for these purposes.

Whilst we duly acknowledge ICANN's efforts regarding acknowledge ICANN's efforts regarding data protection and privacy and its openness to continued dialogue, regrettably, neither the 2013 RAA approved by the ICANN Board on 27 June 2013 nor the Draft Specification addresses sufficiently our concerns which were raised in this correspondence between the Working Party and ICANN on the retention periods and data collection.

The Draft Specification defines in more detail the data to be collected, the purposes for which they may be used and the retention periods for which the data are to be kept under the 2013 RAA. This is welcome in that it would offer more transparency. Nevertheless, the 2013 RAA 2 and the Draft Specification continue to fall short of compliance with European data protection law.

The Draft Specification should only require collection of personal data, which is genuinely necessary for the performance of the contract between the Registrar and the Registrant (e.g. billing) or for other compatible purposes such as fighting fraud related to domain name registration. This data should be retained for no longer than is necessary for these purposes. It would not be acceptable for the data to be retained for longer periods or for other, incompatible purposes, such as law enforcement purposes or to enforce copyright.

Processing contrary to these recommendations would be contrary to three key principles of European data protection law set forth in Directive 95/46/EC. It would violate the principle of purpose limitation under Article 6(1)(b) of Directive 95/46/EC, which prohibits the processing of personal data for incompatible purposes<sup>4</sup>, the requirement under Article 7 of the Directive to have an appropriate legal ground for the processing of data, such as contract, consent or the legitimate interest of the controller<sup>5</sup>, and the requirement of proportionality, including the requirement not to retain data 'longer than is necessary for the purposes for which the data were collected or for which they are further processed'

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

(Article 6(1)(e)). These provisions are specifications of the fundamental rights to privacy and the protection of personal data laid down in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.

Retention of personal data originally collected for commercial purposes, and subsequently retained for law enforcement purposes, has been the subject of a recent landmark ruling by the European Court of Justice, which held Directive 2006/24/EC to be invalid, as an unjustified interference with those rights. The Court recognised that the retention of personal data might be considered appropriate for the purposes of the detection, investigation and prosecution of serious crime, but judged that the Directive 'exceeded the limits imposed by compliance with the principle of proportionality'.<sup>7</sup> It is reasonable to expect requirements for retaining personal data to be subject to increasing scrutiny and legal challenges in the EU.

Further, as you are aware, the current European data protection legislation is under reform. The European Parliament voted on 12 March 2014 overwhelmingly in favour of a new General Data Protection Regulation which is designed to replace Directive 95/46/EC and be directly applicable in each of the twenty-eight EU Member States. There is therefore now a more compelling need than ever before for ICANN to apply the waiver of the retention period under the 2013 RAA Data Retention Specification uniformly to all EU Member States as requested in the 'harmonised statement' of the Working Party issued by letter of 6 June 2013.

We would also encourage ICANN, being at the heart of the future of Internet evolution, and in view of its mandate to serve the public interest on a global scale, to take a lead in ensuring that privacy and data protection are embedded by default, when new tools and instruments or new internet policies are designed, for the benefit of all - not just European - Internet users.

On these grounds, we reiterate our recommendations to reduce the data collection and retention requirements in the 2013 RAA 'by default' to what is genuinely necessary for the performance of the contract between the Registrar and the Registrant (e.g. billing), and to limit processing of this data to compatible purposes, such as proportionate measures to fight fraud related to domain name registration. It is possible that the Working Party may wish to provide more details at a later stage.

### **19. Title:** [European Commission Website: Definition and Obligations of Data Controllers](#)

Summarized by: Kleiman

#### European Commission Website: Definition of Data Controllers

The European Commission website provides information to define what is a Data Controller. Data controllers are the persons or entities "which collect and process personal data." Data controllers are also the persons or entities who "determine 'the purposes and the means of the processing of personal data.'" This applies to both public and private sectors.

According to the European Commission, Data controllers must respect the privacy and data protection rights of those whose personal data is entrusted to them. They must:

- collect and process personal data only when this is legally permitted;
- respect certain obligations regarding the processing of personal data;

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

- respond to complaints regarding breaches of data protection rules;
- collaborate with national data protection supervisory authorities.

### European Commission Website: Obligations of Data Controllers

This is a key question about whether ICANN is a data controller under the laws of the European Data Protection Directive. Data Controllers “determine ‘the purposes and the means of the processing of personal data’” and it is a term that applies to both public and private sectors. See Who can collect and process personal data?, [http://ec.europa.eu/justice/data-protection/data-collection/index\\_en.htm](http://ec.europa.eu/justice/data-protection/data-collection/index_en.htm) (summarized above)

The EU Data Protection Directive requires Data Controllers to abide by certain principles when they process personal data. According to the European Commission:

“Each data controller must respect the following rules as set out in the Directive:

Personal Data must be processed legally and fairly;

It must be collected for explicit and legitimate purposes and used accordingly;

It must be adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed;

It must be accurate, and updated where necessary;

Data controllers must ensure that data subjects can rectify, remove or block incorrect data about themselves;

Data that identifies individuals (personal data) must not be kept any longer than strictly necessary;

Data controllers must protect personal data against accidental or unlawful destruction, loss, alteration and disclosure, particularly when processing involves data transmission over networks. They shall implement the appropriate security measures;

These protection measures must ensure a level of protection appropriate to the data.”

Additional information:

It is hard to put it more succinctly, so I have quoted directly from the European Commission webpage.

## **20. Title: [IWG Common Position relating to Reverse Directories \(Hong Kong, 15.04.1998\)](#)**

Summarized by: [Ali](#)

It is in any case necessary to endow the persons with the right to be informed by their provider of telephone or e-mail service, at the time of the collection of data concerning them, or if they have already subscribed, by a specific means of information, of the existence of services of reverse search and

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

- if express consent is not required - of their right to object, free of charge, to such a search.

### 21. Title: [IWG Common Position on Privacy and Data Protection aspects of the Registration of Domain Names on the Internet \(Crete, 4./5.05.2000\)](#)

Summarized by: [Ali](#)

The Working Group notes that the "Working Party on the protection of individuals with regard to the processing of personal data" of Data Protection Commissioners in the European Union ("Article 29 Group") has addressed these issues extensively in their "Opinion 3/99 on Public Sector information and the Protection of Personal Data" and fully supports their findings.

### 22. Title: [IWG Common Position on Privacy and Data Protection aspects of the Publication of Personal Data contained in publicly available documents on the Internet \(Crete, 4./5.05.2000\)](#)

Summarized by: [Ali](#)

- The amount of data collected and made publicly available in the course of the registration of a domain name should be restricted to what is essential to fulfil the purpose specified. In this respect the Working Group has reservations against a mandatory publication of any data exceeding name (which might also be the name of a company and not of a natural person), address and e-mailaddress in cases where the domain name holder is not himself responsible for the technical maintenance of the domain but has this done through a service provider (as is the case with many private persons who have registered domain names).
- Any technical mechanism to be introduced to access the data collected from the registrants must furthermore have safeguards to meet the principle of purpose limitation and avoidance of the possibility to unauthorised secondary use of the registrant's data.

### 23. Title: [IWG Common Position on Incorporation of telecommunications-specific principles in multilateral privacy agreements: Ten Commandments to protect Privacy in the Internet World \(Berlin, 13/14.09.2000\)](#)

Summarized by: [Ali](#)

Data Austerity: Telecommunications infrastructure has to be designed in a way that as few personal data are used to run the networks and services as technically possible.

Virtual Right to be Alone: Nobody must be forced to let his or her personal data be published in directories or other indices. Every user has to be given the right to object to his or her data being collected by a search engine or other agents. Every user has to be given the right and the technical means to prevent the intrusion of external software into his own devices.

**24. Title: [IWG Common Position on data protection aspects in the Draft Convention on cyber-crime of the Council of Europe \(Berlin, 13/14.09.2000\)](#)**

Summarized by: [Ali](#)

In this respect the Working Group fully supports the findings of the European Data Protection Commissioners Conference that such retention of traffic data by Internet service providers would be an improper invasion of the fundamental rights guaranteed to individuals by the European Convention on Human Rights. This goes also for storing data revealing the use of the Internet by individuals. Existing powers for tracing crimes should not be extended in a way that invades privacy until the need for such measures has been clearly demonstrated. The Working Group has in the past stated that any Interception of Private Communications should be subject to appropriate safeguards.

**25. Relevant National Laws that may apply to gTLDs, including [U.S. Anticybersquatting Consumer Protection Act \(ACPA\), 15 USC §1125](#)**

Summarized by: [Aaron](#)

There are national laws that address the registration and use of gTLD domain names. These laws assume that registrants can be identified via registration data.

An example is the [U.S. Anticybersquatting Consumer Protection Act \(ACPA\), 15 USC §1125\(D\)](#). This law "was intended to prevent 'cybersquatting,' an expression that has come to mean the bad faith, abusive registration and use of the distinctive trademarks of others as Internet domain names, with the intent to profit from the goodwill associated with those trademarks." (Shields v. Zuccarini, 254 F3d 476 3d Cir. 2001) The ACPA is used to contest the registration of gTLD domains.

The ACPA assumes that the identity of the registrant is established via registration records provided by the registrar: "A person shall be liable for using a domain name under subparagraph (A) only if that person is the domain name registrant or that registrant's authorized licensee." The ACPA also states that the plaintiff may send a notice of the alleged violation and intent to proceed under legal process "to the registrant of the domain name at the postal and e-mail address provided by the registrant to the registrar." The law also requires that "Documents sufficient to establish control and authority regarding the disposition of the registration and use of the domain name" must also be deposited with the court.

[NOTE to WG: Does anyone know of other national laws that apply to gTLD names? Please insert here. I googled a bit but did not find any readily. The Danish Domain Name Act is applicable to .DK domains only, the French Post and Electronic Communications Code (CPCE) applies to .FR and .RE domains only, Belgium's Act on Cybersquatting is for .BE domains only, and the Finnish Domain Nama Act applies to .FI domains only.)

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

### 26. Title: [EWG Recommendations for a Next-Generation RDS, especially](#)

Section 3, Users and Purposes, Annex C, Example Use Cases, Annex A, Board Questions

Summarized by: [Prosser](#)

#### Section 3, Users and Purposes

\*\*\*Although the EWG did not attempt to identify all possible use cases, it endeavoured to explore a representative sample in hopes of rigorously identifying kinds of users and their purposes in wanting access to gTLD registration data. However, the RDS must be designed with the ability to accommodate new users and permissible purposes that are likely to emerge over time." \*\*\*(Page 26)\*

The EWG's [re]prt did summarize "permissible" purposes the EWG identified at the time. The purposes identified are listed below. For brevity of email, I did not include the full definitions. They can be found in Section III, Table 2 Purpose Definitions, Pages 26-27.

#### Purpose:

- Domain Name Control
- Personal Data Protection
- Technical Issue Resolution
- Domain Name Certification
- Individual Internet Use
- Business Domain Name Purchase or Sale
- Academic / Public Interest DNS Research
- Legal Actions
- Regulatory and Contractual Enforcement
- Criminal Investigation & DNS Abuse Mitigation
- DNS Transparency

It should be noted the EWG identified an additional purpose, Malicious Internet Activities, which it did not further include in the "permissible" purposes.

#### Annex C, Example Use Cases

Using the same permissible purpose listing provided in Section III, Annex C included examples of specific uses for clarity. For example Domain Name Control is required in registration and transfer, among other purposes OR Regulatory and Contractual Enforcement for UDRP proceeding and Tax investigations. The full list of example use cases along with a specific example of Technical Issue Resolution purpose is available on Pages 126-128.

#### Annex A, Board Questions, Pages 123-124

\*"The Board resolution that directed the EWG's work included a series of specific questions to be answered as it conducted its analysis. This Annex references the sections of this Report that address the Board's concerns."\*

The initial question presented to EWG was by the Board was:

EWG to redefine the purpose of:

- collecting,
- maintaining, and



## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

- providing access to gTLD registration data, and
- consider safeguards for protecting data

This was addressed in Section III, Users & Purposes and Section VI, Improving Accountability (presented above in email). In addition, Section III addressed the following Board Questions that were around use and purpose of data. I included them as a reference point to raise awareness of Board concerns in clarifying various use cases and purposes:

- Why are data collected?
- Who needs the data and why?
- Law enforcement access to details about a domain name registration?
- Intellectual property owner access to details about a domain name registration?
- Security practitioner access to details about a domain name registration?
- What value does the public realize with access to registration data?
- What comprises a legitimate law enforcement need?
- What registration data and to what level of accuracy comprises valuable information to a law enforcement agent that is looking for the real identity of the responsible party?
- Is the desired domain name registration data access consistent with access that intellectual property owners have to similar types of data in other industries?
- Of all the registration data available, what does an intellectual property owner need access to?

A separate question: What purpose will the data serve? Was addressed in ANNEX D: PURPOSES AND DATA NEEDS, Pages 129-132

Annex D defined the registration data element and mapped it to Purposes defined by EWG in Section III, Table 2 with Section VI(a) Data Elements. This reference is useful for specific currently defined registration data elements purposes.

Also summarized by [Vayra](#)

- Purpose is mentioned 25 separate times throughout the report, including in the overall EWG recommendation for "a paradigm shift to a next-generation RDS that collects, validates and discloses gTLD registration data for permissible purposes only. While basic data would remain publicly available, the rest would be accessible only to accredited requestors who identify themselves, state their purpose, and agree to be held accountable for appropriate use."  
...  
"The EWG is confident that this Final Report fulfills the ICANN Board's directive to help redefine the purpose and provision of gTLD registration data, providing a solid foundation to help the ICANN community (through the Generic Names Supporting Organization, GNSO) create a new global policy for gTLD directory services."
- See in more detail Sections on Purpose, specifically: II(b) Purpose, III(b) RDS Users and Purposes, III(c) Purposes to be Accommodated or Prohibited, III(e) Purpose-Based Contact Principles, III(f) Purpose-Based Contact Roles and Responsibilities

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

### 27. Materials: EWG Tutorials and FAQs

[EWG Tutorial](#) Pages 17-20, 37-41

[EWG FAQs](#) 9-12, 67

Video FAQ "[Is my purpose supported by the RDS?](#)"

Summarized by: [Prosser](#)

[EWG Tutorial, Pages 17-20, 37-41](#)

Slides, associated audio, & transcript:

- <http://london50.icann.org/en/schedule/mon-ewg-final-overview/presentation-ewg-final-overview-23jun14-en.pdf>
- <http://audio.icann.org/meetings/london2014/ewg-final-overview-23jun14-en.mp3>
- <https://london50.icann.org/en/schedule/mon-ewg-final-overview/transcript-ewg-final-overview-23jun14-en>

Page 17

This page presents the purposes surfaced through EWG work. It is noted in the audio and on the presentation the purposes presented may not meet \*all\* use cases. Any solution must be flexible to allow for future purpose needs.

Page 18

Recognition is made every permissible purpose as data needs, but they vary. Some may be widely used with minimal control standards whereas others will require higher scrutiny and authority for access. Also introduced are the potential provisions for whoas (history) or reverse (related domains) queries.

Page 19

Purpose based contact (PBC) is a proposal to offer better control of personal information and more efficient portability of contact data.

Page 20

Workflow example of Gate access in a legal action is presented. It walks through how the process would operate with authentication service. If the requestor was authorized for access and to what level, then provide data only relevant to their need and their approval level.

Page 21

Presentation page contains what could be in PBC data, noting that PBC may still be a proxy service. It offers users choices to determine what they want for contact information, what information willing to share at what level, and ability to update information once not across multiple platforms.

(not on audio or transcript I could find):

Page 38

Provides a chart with identified Purpose and associated Task for each.

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

Page 39

Purposed Based Contacts (PBC) examples are provided as backup to the presentation. The EWG supplied three specific examples of use as Individual using own data, Individual or Org using a Privacy service and a Business using 3rd party PBC.

Page 40

The table of Purposes and Needs is provided as backup to the presentation. The table defines the query scope, type of contacts needed based on purpose, registrant data availability level and other queries that may be needed for specific purposes, such as Reverse and WhoWas.

Page 41

The PBC and their responsibilities are defined and provided as backup to the presentation. These are the proposed referenced throughout the presentation.

### Expert Working Group on gTLD Directory Services (EWG) Frequently Asked Questions (FAQs) – 2014 Final Report Update

Five (5) FAQ's specifically addressed Purpose, captured below. (Page 5)

\*Registration Data Users and Purposes \*

9) Who are the users of the RDS? How did the EWG determine this?

The EWG analyzed previous reports and use cases to identify users who want access to gTLD registration data, including registrants, protected registrants, on-line service providers, business Internet users, intellectual property owners, law enforcement agencies and OpSec staff, Internet technical staff, individual Internet users, Internet researchers, non-LEA investigators of malicious activity, the general public, and bad actors.

10) Why do those users need access to registration data?

Use cases also shed light on rationale and purposes served by gTLD registration data, including domain name control, regulatory/contract enforcement, academic/public interest domain name research, domain name purchase/sale, personal data protection, individual Internet use, technical issue resolution, domain name certification, legal action, regulatory and contractual enforcement, criminal investigation and DNS abuse mitigation, DNS transparency, and malicious Internet activities.

11) Which purposes should not be permissible?

Given no rationale for accommodating the needs of some users but not others that access WHOIS today, the EWG recommended the RDS accommodate all non-malicious uses.

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

12) Why didn't the EWG consider user X or purpose Y?

Use cases examined by the EWG were not exhaustive, but representative enough of existing and potential uses to establish RDS needs. The EWG also recommended a process for adding new purposes as may be required to address future global Internet needs.

67) How will members of the press and bloggers gain access to RDS data?

The DNS Transparency purpose was intended to cover media needs for registration data. However, if the data available for that permissible purpose does not prove sufficient, the EWG also recommended an on-going process for users to suggest new permissible purposes.

### 28. Title: EWG Member Statement by [Perrin](#)

Summarized by: [Perrin](#)

Perrin dissented from the consensus of the EWG regarding its recommendations, citing three specific concerns:

- 1) Requirement to have a legal contact, address and phone number mandatory to provide, and published outside the gate, in the publically available data.
- 2) Default for simple registrants who don't hire a lawyer or other actor to assume the role of legal contact is publishing registrant information, notably address and phone number in the RDS outside the gate.
- 3) The inclusion of a principle of consent (28), whereby a registrant may consent to the use or processing of her gated information for the permissible purposes enumerated for accredited actors behind the gate. Constitutes coerced consent, unlikely to be able to understand likely implications of consent. Rights under law abrogated.

Accountability does not equal transparency of detailed personal or business information, it means responsiveness. If a registrant fails to respond to serious issues contact the registrar to take action.

Purpose of gated access is sheltering customer data; screen out bad actors from harassing innocent registrants, deter identity theft, and ensure that only legitimate complaints arrive directly at the door of the registrants. Protects ability of registrants to express themselves anonymously. Placing all contact data outside the gate defeats certain aspects of having a gate in the first place.

Proposed mitigations for privacy protection unlikely to work for various reasons:

- 1) Proxy services cost \$\$
- 2) rules engine unproven, difficult to build given lack of sound basis for jurisdictional differentiation

## Purpose Team Summaries - drafted by gnso-rds-pdp-purpose@icann.org

Right of privacy in directory services confirmed by recent court decisions: Supreme Court of Canada:

<http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do>, comparable decision from the US Supreme Court: <http://www.law.cornell.edu/supct/html/93-986.ZO.htm>

### 29. Title: **EWG Member Blog by [Samuels](#)**

Summarized by: [Samuels](#)

In the blog post I implicitly accepted that data acquisition and use of WHOIS data covers a lot of purposeful uses, inclusive of spammers.

I acknowledged that a requirement by the old WHOIS system for publication of so much of the personal data of registrants have had deleterious effects, including providing false and inaccurate data to guard against invasion of privacy.

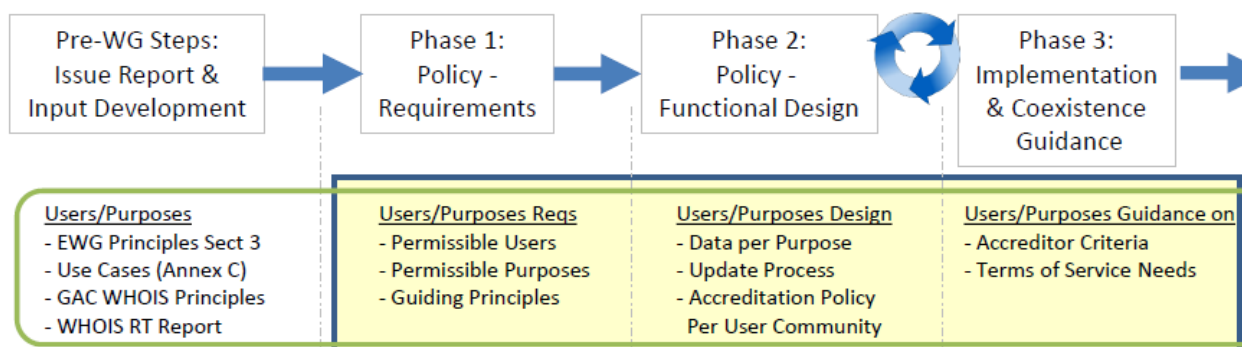
I allowed that in examining the concerns of all stakeholders and classes of users of registration data, the EWG concluded that a 'free for all' approach where everyone has the same public access to registration data was not defensible or any longer desirable.

I endorsed the new approach and vouchsafe satisfaction to all stakeholder classes. I adopted the position that all purposes are not equal. It was progress that for the next generation RDS, we should collect and validate all of the settled elements in RDS dataset. However, beyond a limited subset of that for public consumption, we disclose the rest only for adjudged permissible purposes to an accountable and identifiable set of users.

See the full blog post [here](#).

### 30. Title: **[Process Framework](#) for a PDP on Next-Generation RDS**

Summarized by: [Mind Map](#)



See [Mind Map](#) for further detail on above sub-questions associated with this part of the Framework.

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

### 31. Title: [Registrar Accreditation Agreement \(2013\)](#)

Summarized by: [Aaron](#)

#### SUMMARY:

Registration data is collected in order to record the identity of the party that has registered a gTLD domains name. This party is the registrant, or "registered domain-name holder," and has attendant legal rights and responsibilities. ICANN policies require that the name of the sponsoring registrar, the registrant's contact data, and other contact data be published publicly in WHOIS, so that they can be identified by and contacted by various parties for legal purposes. Some national laws assume that domain registrants will be identified through registration data.

[2013 REGISTRAR ACCREDITATION AGREEMENT \(2013 RAA\)](#) defines what a registrant is. It states:

"1.1 "Account Holder" means the person or entity that is paying for the Registered Name or otherwise controls the management of the registered name, when that person or entity is not the Registered Name Holder....

1.16 "Registered Name Holder" means the holder of a Registered Name."

Note that an Account Holder can be the same or different from a domain's Registrant. An Account Holder can create an account at a registrar, and then use that account to register domains names for other registrants. So, the business transaction of making a registration is related to but can also be distinct from being a domain registrant. The 2013 RAA requires that registrars record data about the Account Holders and Registered Name Holders. The identities of Account Holders are not necessarily published in WHOIS -- there is no "Account Holder" contact type. If the Account Holder and Registered Name Holder are one and the same, its data appears in WHOIS in the Registrant Contact fields.

The 2013 RAA contains terms that are binding between the registrant and its registrar, stating legal rights and responsibilities. Among others it states:

"3.7.7 Registrar shall require all Registered Name Holders to enter into an electronic or paper registration agreement with Registrar including at least the provisions set forth in Subsections 3.7.7.1 through 3.7.7.12, and which agreement shall otherwise set forth the terms and conditions applicable to the registration of a domain name sponsored by Registrar.... Registrar shall use commercially reasonable efforts to enforce compliance with the provisions of the registration agreement between Registrar and any Registered Name Holder that relate to implementing the requirements of Subsections 3.7.7.1 through 3.7.7.12 or any Consensus Policy."

### 32. Title: [WHOIS Uniform Domain Name Dispute Resolution Policy and Rules for Uniform Domain Name Dispute Resolution Policy](#)

Summarized by: [Aaron](#)

Through the contracts, the registrant has rights and responsibilities under ICANN policies, and under any applicable registry and registrar policies. Among those, all gTLD registrants are bound to the Uniform Dispute Resolution Policy (UDRP). Registrants of new gTLD domains are also bound to the Uniform Rapid Suspension policy, or URS. Registrants may also have legal rights and responsibilities under local laws.

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

Under ICANN policy, contact data published in WHOIS is required to administrate UDRP and URS cases. The UDRP and URS policies assume that the contact data is published publicly, where potential complainants can see it.

The [Uniform Domain Name Dispute Resolution Policy](#) states as follows:

"1. Purpose. This Uniform Domain Name Dispute Resolution Policy (the "Policy") has been adopted by the Internet Corporation for Assigned Names and Numbers ("ICANN"), is incorporated by reference into your Registration Agreement, and sets forth the terms and conditions in connection with a dispute between you and any party other than us (the registrar) over the registration and use of an Internet domain name registered by you.

2. Your Representations. By applying to register a domain name, or by asking us to maintain or renew a domain name registration, you hereby represent and warrant to us that (a) the statements that you made in your Registration Agreement are complete and accurate; (b) to your knowledge, the registration of the domain name will not infringe upon or otherwise violate the rights of any third party; (c) you are not registering the domain name for an unlawful purpose; and (d) you will not knowingly use the domain name in violation of any applicable laws or regulations. It is your responsibility to determine whether your domain name registration infringes or violates someone else's rights."

The accompanying [Rules for Uniform Domain Name Dispute Resolution Policy](#) (the "Rules") state:

"Registrar means the entity with which the Respondent has registered a domain name that is the subject of a complaint.

Registration Agreement means the agreement between a Registrar and a domain-name holder.

Respondent means the holder of a domain-name registration against which a complaint is initiated."

The UDRP Rules then require that official communications be sent to the contacts published in WHOIS, specifically the Registrant, Administrative, and Technical contacts:

"2. Communications

(a) When forwarding a complaint, including any annexes, electronically to the Respondent, it shall be the Provider's responsibility to employ reasonably available means calculated to achieve actual notice to Respondent. Achieving actual notice, or employing the following measures to do so, shall discharge this responsibility:

(i) sending Written Notice of the complaint to all postal-mail and facsimile addresses (A) shown in the domain name's registration data in Registrar's Whois database for the registered domain-name holder, the technical contact, and the administrative contact and (B) supplied by Registrar to the Provider for the registration's billing contact; and

(ii) sending the complaint, including any annexes, in electronic form by e-mail to:

(A) the e-mail addresses for those technical, administrative, and billing contacts;...

(e) Either Party may update its contact details by notifying the Provider and the Registrar."

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

### 33. Title: WHOIS New gTLD [URS Policy](#) and [Rules for URS Policy](#)

Summarized by: [Aaron](#)

The [URS](#) contains similar requirements to use domain contact data published in WHOIS:

"[The Complaint will contain the following:]

1.2.3 Name of Registrant (i.e. relevant information available from Whois) and Whois listed available contact information for the relevant domain name(s).

1.2.4 The specific domain name(s) that are the subject of the Complaint. For each domain name, the Complainant shall include a copy of the currently available Whois information and a description and copy, if available, of the offending portion of the website content associated with each domain name that is the subject of the Complaint....

4.2 Within 24 hours after receiving Notice of Lock from the Registry Operator, the URS Provider shall notify the Registrant of the Complaint ("Notice of Complaint"), sending a hard copy of the Notice of Complaint to the addresses listed in the Whois contact information, and providing an electronic copy of the Complaint....

4.3 The Notice of Complaint to the Registrant shall be sent through email, fax (where available) and postal mail. The Complaint and accompanying exhibits, if any, shall be served electronically."

The [URS Rules](#) state:

"2. Communications

(a) When forwarding a Complaint, including any annexes, electronically to the Respondent, it shall be the Provider's responsibility to employ reasonably available means calculated to achieve actual notice to Respondent. Achieving actual notice, or employing the following measures to do so, shall discharge this responsibility:

(i) sending the Notice of Complaint to all email, postal mail and facsimile addresses shown in the domain name's registration data in the Whois database for the registered domain-name holder, the technical contact, and the administrative contact, as well as to any email addresses for the Respondent provided by the Complainant..."

### 34. Title: WHOIS [Expired Domain Deletion Policy](#)

Summarized by: [Aaron](#)

The [Expired Domain Deletion Policy](#) is Consensus Policy which requires that registrant data be published in WHOIS and handled in a certain way during UDRP disputes:

"3.7.5.7 In the event that a domain which is the subject of a UDRP dispute is deleted or expires during the course of the dispute, the complainant in the UDRP dispute will have the option to renew or restore the name under the same commercial terms as the registrant. If the complainant renews or restores the name, the name will be placed in Registrar HOLD and Registrar LOCK status, the WHOIS contact information for the registrant will be removed, and the WHOIS entry will indicate that the name is subject to dispute."



## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

### 35. Title: WHOIS [Inter-Registrar Transfer Policy](#)

Summarized by: [Aaron](#)

The newest version of the [Inter-Registrar Transfer Policy](#) became Consensus Policy in 2015 and takes effect on 1 August 2016. A [slightly different version](#) became effective 31 January 2015.

The policy is a set of requirements regarding the transfer of domains from one sponsoring registrar to another. A purpose of the policy is to prevent transfers that have not been authorized by the domain holder (including malicious "domain hijackings"). As such, the Policy defines who has rights to the domain, and states that only Administrative Contacts and the Registered Name Holders (Registrant contacts) may authorize transfers. The Policy states that these contacts must be published in the publicly-accessible WHOIS.

The version of the Policy taking effect on 1 August 2016 says:

#### "1.1 Transfer Authorities

The Administrative Contact and the Registered Name Holder, as listed in the Losing Registrar's or applicable Registry's (where available) publicly accessible Whois service are the only parties that have the authority to approve or deny a transfer request to the Gaining Registrar. In the event of a dispute, the Registered Name Holder's authority supersedes that of the Administrative Contact.

Registrars may use Whois data from either the Registrar of Record or the relevant Registry for the purpose of verifying the authenticity of a transfer request; or from another data source as determined by a consensus policy....

2.1.2 In the event that the Gaining Registrar relies on a physical process to obtain this authorization, a paper copy of the FOA will suffice insofar as it has been signed by the Transfer Contact and further that it is accompanied by a physical copy of the Registrar of Record's Whois output for the domain name in question....

2.2.1 Transmission of a "transfer" command constitutes a representation on the part of the Gaining Registrar that the requisite authorization has been obtained from the Transfer Contact listed in the authoritative Whois database....

3.6 In the event that a Transfer Contact listed in the Whois has not confirmed their request to transfer with the Registrar of Record and the Registrar of Record has not explicitly denied the transfer request, the default action will be that the Registrar of Record must allow the transfer to proceed.

#### II.B. Availability of Change of Registrant

1.1 In general, registrants must be permitted to update their registration/Whois data and transfer their registration rights to other registrants freely."

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

### 36. ICANN WHOIS Portal Knowledge Center Q&A: [What is WHOIS data used for?](#)

Summarized by: [Aaron](#)

Quoted from this page is on the ICANN web site: <https://whois.icann.org/en/what-whois-data-used>

WHOIS is indispensable to the smooth operation of the DNS and is used for many legitimate purposes, including:

- To contact network administrators for resolution of technical matters related to networks associated with a domain name (e.g., DNS or routing matter, origin and path analysis of DoS and other network-based attacks).
- To diagnose registration difficulties. WHOIS queries provide information that is often useful in resolving a registration ownership issue, such as the creation and expiration dates and the identity of the registrar.
- To contact web administrators for resolution of technical matters associated with a domain name.
- To obtain the real world identity, business location and contact information of an online merchant or business, or generally, any organization that has an online presence.
- To associate a company, organization, or individual with a domain name, and to identify the party that is operating a web or other publicly accessible service using a domain name, for commercial or other purposes.
- To contact a domain name registrant for the purpose of discussing and negotiating a secondary market transaction related to a registered domain name.
- To notify a domain name registrant of the registrant's obligation to maintain accurate registration information.
- To contact a domain name registrant on matters related to the protection and enforcement of intellectual property rights.
- To establish or look into an identity in cyberspace, and as part of an incident response following an Internet or computer attack. (Security professionals and law enforcement agents use WHOIS to identify points of contact for a domain name.)
- To gather investigative leads (i.e., to identify parties from whom additional information might be obtained). Law enforcement agents use WHOIS to find email addresses and attempt to identify the location of an alleged perpetrator of a crime involving fraud.
- To investigate spam, law enforcement agents look to the WHOIS database to collect information on the website advertised in the spam.

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

### 37. Title: [Privacy & Information Security Law Blog: Article 29 Working Party Clarifies Purpose Limitation Principles](#)

Summarized by: Kleiman

Source: Privacy & Information Security Law Blog, Hunton & Williams law firm.

Date: April 9, 2013 (see heading above for Title and Hyperlink to Blog)

This blog piece summarizes the Article 29 Working Party “Opinion 03/2013 on Purpose” for a general audience. (The Article 29 Working Party includes the Data Protection Commissioners of each country in the EU.) This Opinion explains “the purpose limitation principle” of the EU Data Protection Directive as having two parts:

- (1) the requirement that processing must be for a specified, explicit and legitimate purpose; and
- (2) the requirement that any further processing must be compatible with the original purpose for which the personal data were collected.

To process “for a specified, explicit and legitimate purpose,” the blog notes that Article 29 WG wrote that vague purpose statements such as “improving user experience” or “marketing purposes” will usually not suffice.

To process personal data for purposes other than those for which it was originally collected, the Working Party wrote that a case-by-case analysis is needed to see whether that further processing would be compatible with the original purpose? In this assessment, the Article 29 WP wrote there are four factors to take into consideration:

- “the relationship between the purposes for data collection and the purposes for further processing;
- the context in which the data have been collected and the reasonable expectations of the data subjects regarding further use of the data;
- the nature of the data and the impact of the further processing on the data subjects; and
- the safeguards put in place by the data controller to ensure fair processing and prevent undue harm to data subjects.”

The blog piece notes that Annex 4 of the Opinion contains specific examples of how this assessment might work.

Re: “Big Data,” Hunton & Williams wrote that when processing “Big Data” that directly affects individuals, the Article 29 WP found that “specific opt-in consent will almost always be necessary.”

Additional Information: This summary references [Title: Article 29 WP 203 Opinion 3/2013 Opinion on Purpose](#), decided by the EU's Article 29 Working Party, also summarized in this document.

**38. Title: [U.S. NTIA Green Paper: Improvement of Technical Management of Internet Names and Addresses \(1998\)](#)**

Summarized by: [Vayra](#) (p8)

- The job of policing trademarks could be considerably easier if domain name databases were readily searchable through a common interface to determine what names are registered, who holds those domain names, and how to contact a domain name holder. Many trademark holders find the current registration search tool, who is, too limited in its functioning to be effective for this purpose. A more robust and flexible search tool, which features multiple field or string searching and retrieves similar names, could be employed or developed to meet the needs of trademark holders. The databases also could be kept up to date by a requirement that domain name registrants maintain up-to-date contact information.

- Appendix 2--Minimum Dispute Resolution and Other Procedures Related to Trademarks

1. Minimum Application Requirements.

a. Sufficient owner and contact information (e.g., names, mail address for service of process, e-mail address, telephone and fax numbers, etc.) to enable an interested party to contact either the owner/applicant or its designated representative

...

2. Searchable Database Requirements.

a. Utilizing a simple, easy-to-use, standardized search interface that features multiple field or string searching and the retrieval of similar names, the following information must be included in all registry databases, and available to anyone with access to the Internet:

- Up-to-date ownership and contact information;
- Up-to-date and historical chain of title information for the domain name;
- A mail address for service of process;
- The date of the domain name registration; and
- The date an objection to registration of the domain name was filed.

3. Updated Ownership, Contact and Use Information.

a. At any time there is a change in ownership, the domain name owner must submit the following information:

- Up-to-date contact and ownership information; and
- A description of how the owner is using the domain name, or, if the domain name is not in use, a statement to that effect.

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

### 39. Title: [U.S. NTIA White Paper: Management of Internet Names and Addresses, Statement of Policy \(2012\)](#)

Summarized by: [Vayra](#) (p9)

Trademark Issues. Trademark holders and domain name registrants and others should have access to searchable databases of registered domain names that provide information necessary to contact a domain name registrant when a conflict arises between a trademark holder and a domain name holder. To this end, we anticipate that the policies established by the new corporation would provide that following information would be included in all registry databases and available to anyone with access to the Internet:

§ up-to-date registration and contact information;

§ up-to-date and historical chain of registration information for the domain name;

§ a mail address for service of process;

§ the date of domain name registration;

§ the date that any objection to the registration of the domain name is filed; and

§ any other information determined by the new corporation to be reasonably necessary to resolve disputes between domain name registrants and trademark holders expeditiously.

### 40. Title: [U.S. GAO INTERNET MANAGEMENT: Prevalence of False Contact Information for Registered Domain Names \(2005\)](#)

Summarized by: [Aaron](#)

"The Whois service was originally intended as a source of contact information that technicians could use to reach each other when necessary to troubleshoot problems with Internet connectivity or functionality. However, users of the Whois service have broadened over time to include law enforcement officials, owners of intellectual property, and others seeking contact information about Web site owners for a variety of reasons." (page 4)

"Created in the 1970s, Whois began as a service that Internet operators could use to identify and contact individuals or entities responsible for the operation of a computer on the Internet when an operational problem arose. Since then, the Whois service has evolved into a tool used for many purposes, such as determining whether a domain name is available for registration, identifying the source of spam e-mail, enforcing intellectual property rights, and identifying and verifying online merchants." (page 19)

"Data accuracy is important to the effectiveness of the Whois service in helping Internet operators to resolve technical network issues, as well as helping law enforcement officers to investigate such things as intellectual property misuse or online fraud. According to federal agency officials, accurate Whois data have the potential to allow law enforcement officials to identify individuals involved in criminal

## Purpose Team Summaries - drafted by [gns0-rds-pdp-purpose@icann.org](mailto:gns0-rds-pdp-purpose@icann.org)

activities on the Internet more quickly than if such information were not available." (page 20)

### 41. Title: [Anti-Phishing Working Group Advisory on Utilization of Whois Data For Phishing Site Take Down \(2008\)](#)

Summarized by: [Aaron](#)

"Given fundamental policy changes regarding accessibility of both domain and IP Whois data currently under consideration by ICANN, RIPE and others, and the evolving environment surrounding the Whois system, the APWG Internet Policy Committee (IPC) has updated this industrial advisory, comprised of a set of real-world case studies in which Whois data has been instrumental in neutralizing phishing sites in order to help ICANN, RIPE and others comprehensively inform their policy deliberations. The intent is to better inform the broader internet policy community of the invaluable assistance the full range of Whois data provides in shutting down nearly 1,000 phishing sites per day (and climbing) at current rates....

In a majority of phishing cases, published Whois data of the domain name(s) and Internet Protocol (IP) network addresses involved have been irreplaceable components of the take down process -- invaluable resources, in fact, necessary to the resolution of most of the cited cases. For cases in which legitimate machines or services have been hacked or defrauded, published domain name or IP network address Whois information is an important tool used to quickly locate and communicate with site owners and service providers. For cases in which domain names are fraudulently registered, the published domain name Whois information can often be tied to other bogus registrations or proven false to allow for quick shut down....

It is the hope of the APWG's IPC that exposure to this information and the following case studies will allow the relevant committees of ICANN, RIPE and other governance bodies to make better informed decisions on Whois policy and promote policy modifications that will not result in reduced access to Whois data for those who use it to respond to phishing events....

In all, over 80% of phishing site take-downs involve using the domain name Whois system to find a contact for assistance via e-mail, phone and/or fax, or to prove the registration to be fraudulent through any or all portions of the available Whois information."